BLOCKCHAIN

TÜRKİYE

DIGITAL ID

Blockchain Turkey Platform, Finance, Banking And Insurance Working Group Report

APRIL 2019

TBV

TÜRKİYE BİLİŞİM VAKFI

DIGITAL ID

Blockchain Turkey Platform, Finance,
Banking And Insurance Working Group Report

APRIL 2019

All information and opinions in this Report belong to its authors, and do not represent the opinions of the Blockchain Turkey Platform. The content of this Report can be modified anytime without any notifications on the website by its authors.

***

Design and Graphic Works
TERMİNAL MEDYA LTD. ŞTİ.
Maslak Mah. Bilim Sokak No:5 SUN Plaza Kat:13 Sarıyer/İSTANBUL
0(212) 367 4988 ve 0(532)643 6959

Editor
ÖZLEM ÖZKAN

Graphic Works
GÜLİSTAN ŞENOL

Printing
SET POZİTİF MATBAACILIK
Maslak Mah. Ahi Evran Cad. Rentaş İş Mrkz.
A Blok No: 62 Sarıyer/İSTANBUL
0(212) 286 4933

Finance, Banking and Insurance

DISCLAIMER

"This report prepared by the "Manufacturing, Logistics and Transportation Working Group" of Blockchain Turkey Platform operating under Turkish Informatics Foundation has been prepared to to offer solutions for solving the problems encountered in the management of this report provide chain is for informational purposes only, people and institutions binding recommendations or opinions does not qualify. This report contains information from publicly available sources and is not guaranteed to be up-to-date and complete. All information and opinions given in this report may change in time. Within this context, this report has no responsibilities or obligations against individuals reading its content or any third parties."

CONTENTS

TBV
TÜRKİYE BİLİŞİM VAKFI

Turkish Informatics Foundation (TBV) *was founded with the aim of transforming Turkey into an information society by contributing to the development of the required infrastructure and increasing the share of information technology in the country's economy by pursuing economic and social studies, undertaking scientific R&D, creating relevant projects and ensuring their application.*

BLOCKCHAIN
TÜRKİYE

The Blockchain Turkey Platform *was founded with the aim of creating a sustainable blockchain ecosystem in Turkey and alleviating the difficulties in the new modes of conducting business by creating a sharing platform, both led by the Turkish Informatics Foundation (TBV).*

PREFACE

Faruk Eczacıbaşı
Turkish Informatics Foundation (TBV)
Chairman of the Board

When we founded Turkish Informatics Foundation (TBV) in 1995, it had a simple mission: Leverage information and communications technologies to increase the country's productivity. Call it Industry 4.0 or the information society, the world has entered a period of acceleration, forcing us to change our thinking.

Blockchain is likely to be one of the most transformative products of this new line of thinking and further experience is needed for it to be properly understood and applied. As in every new technology, blockchain needs to evolve from the experimental stage, which involves conceptual thinking, to the pilot stage and on to the final product.

Blockchain's dependence on collaboration, which manifests itself in settings such as inter-industry consortia and other platforms, sets it apart from other technologies. Blockchain gives prominence to ecosystems, especially those that create value through collaboration instead of comprising individual companies with their own products.

Accordingly, as Turkish Informatics Foundation, we took action on 8 June 2011. We launched the Blockchain Turkey Platform (BCTR) to increase the prevalence of, awareness about and usage of blockchain in Turkey and to identify blockchain's strategic priorities. BCTR is a sharing platform which aims to alleviate the difficulties in the new ways of conducting business by creating a sustainable blockchain ecosystem.

I sincerely hope that, as the world migrates from the "build and sell" business model - to which we've grown accustomed since the invention of the steam machine - to the "co-create & presume" way of thinking, this platform and its work are beneficial for our country.

CONTRIBUTING INSTITUTIONS

accenture

AKBANK

alBaraka

ANADOLU SİGORTA

AVIVA SA

BKM
BANKALARARASI
KART MERKEZİ

Deloitte.

EGÜVEN
Elektronik Bilgi Güvenliği A.Ş.

Ford
FORD OTOSAN

Garanti BBVA

TÜRKİYE İŞ BANKASI

Koçfinans

KoçSistem

KUVEYTTÜRK
SAĞLAM BANKACILIK

Microsoft

SRP|legal
strateji regülasyon politika

softtech

Tansel

TEB

TURKCELL

TÜBİTAK
BİLGEM

VakıfBank

YapıKredi

INTRODUCTION

Dilnişin Bayel

Accenture Turkey

Country Director

At numerous points in our lives, we need to register our details and introduce ourselves to gain access to a service. Similarly, many companies can perform transactions only after their customer has been registered and verified.

Identification has moved far beyond being a mere piece of record given at birth; the definition of ID cards and self-identifying information have broadened over time and an increasing amount of data can now be used to identify a person. Furthermore, the definition of self-identifying information can change from one service provider to another and an increasing amount of data can now be used to personalize services in the digital world.

In this report, we present an approach to the concept of digital IDs, their implementation and their use in the registration and verification processes that take place between a service provider and a customer. We suggest that a one-time verification allow a user to access the system upon confirmation of this information. We have tried to design a setup in which the user is at the centre and can control what information to provide and with whom.

I would like to thank the whole BCTR Finance, Banking and Insurance team for their contributions. As the Blockchain Turkey Platform, we are very happy to present you with the following report.

EXECUTIVE SUMMARY

From the moment they're born, people possess a set of unique identifiers, which tends to get larger over time. In fact, a new identity is created every time a person registers on a different platform. In the past, people's appearance and people who could identify them were sufficient methods of self-identification but as nation states and international borders came into being, a need for more formal means of identification - such as physical documents like ID cards, driving licenses, passports and bills - arose and people began to use these documents to identify themselves.

In recent years, there has been an increasing need for people to identify themselves in different places, which can be an arduous task due to the difficulties of sharing physical documents and the associated time loss, a risk of oversharing information, the difficulty of verifying the information and the security vulnerabilities that arise from having to share the information (in written or verbal form).

In the modern world, digital IDs have been created to reap the benefits of digitalization and it has now become possible for a person to digitalise processes such as registration and application by digitally sharing their ID with different institutions. In fact, after the initial registration, the same source of information can be used for verification in different transactions.

The report explains why the use of digital IDs is important and identifies the necessary stakeholders based on use cases to make such an ecosystem work. As mentioned in the report, there is a place for digital IDs in all sectors and digital IDs can have even greater impact if stakeholders from the public sphere and the private sector come together.

This report focuses on natural persons and covers digital IDs from a general perspective. There are many different digital ID-based solutions being developed and many different types of infrastructure being used for digital IDs around the world. This report covers the fundamental principles and components needed for digital ID projects. The following is a list of benefits Turkey is expected to gain through the creation of a digital ID ecosystem:

- The ability to identify oneself using mobile devices
- The quick, easy and safe transmission of verified information to natural and legal persons
- In line with the "as-needed" principle, increased privacy through the users' ability to determine the specifics of the information they share and duration for which the information is shared
- Time-saving through the fast transmission of users' verified information
- The confidentiality, safety and integrity of data, made possible through the use of a decentralized structure

Based on global examples, design principles and ID management models, the use of a decentralized collaboration model to manage digital ID services seems inevitable in order to ensure a sustainable digital ID project. It is our greatest hope that the collective method of working seen in Turkey in other sectors be implemented in the digital ID space and allow us to move towards a more digital Turkey.

1. WHAT IS AN ID?

An ID comprises the uniquely-identifying characteristics and distinctive behaviours of a person, including the person's biographic and biologic attributes.

1.1. Steps in the identification process

›› **Identification:** The act of identifying who a person is and is not

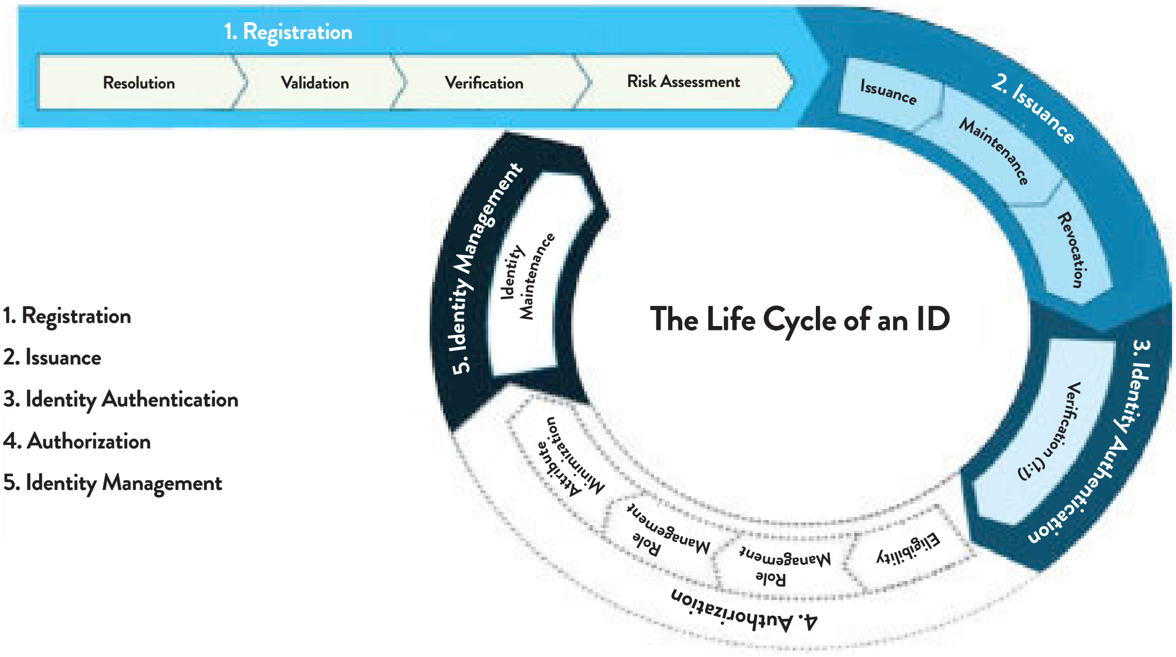
›› **Identification verification:** Using proof and evidence to verify the identity of a person who is seeking to gain access to a service

›› **Authorization:** Upon identification verification, providing a person with access to select services and sources for a specified duration of time and under pre-determined conditions

1.2. The Life Cycle of an ID

The life cycle of an ID actively covers a person's life span and passively covers the period of time after a person's death. In the life cycle, the relevant authorities give / assign the self-identifying information that is used in verifying the identity of a person. (Graphic 1).[1][2]

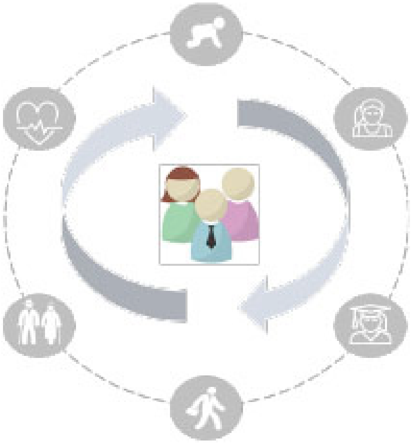
Graphic 1. **The Life Cycle of an ID**[1]



[1] Technology Landscape for Digital Identification, 2018 - World Bank Group.

[2] G20 Digital Identity Onboarding, 2018 - World Bank Group.

The ID life cycle starts with the registration of a person upon their birth, which is the first and foremost step in the ID life cycle. The subsequent steps are updated whenever there is a change in the person's attributes, such as educational qualifications, marriage, divorce, driving license and various legal statuses.



2. DIFFICULTIES RELATED TO PROOFS-OF-IDENTITY

We use many different physical documents in our daily lives to prove our identity. For example, we present self-identifying documents, such as ID cards and bills in our name, to open a bank account at a bank branch, get a phone contract from a mobile provider or check in at our accommodation. In a study conducted in Turkey in 2018[1], the main issues people encounter while providing physical documents to identify themselves were identified as follows:

›› The hassle and time loss associated with providing physical documents and engaging in multiple ID-verification transactions

›› The inability to access required information quickly

›› The oversharing of information

›› The security vulnerabilities that arise from openly sharing identification information (in written or verbal form)

›› The inability to know what happens to shared information or how it is stored

›› The need to create a new ID for every new service

›› Having a multitude of digital IDs (usernames, passwords) to manage and remember

›› Having copious physical identification documents to store and carry

Using digital IDs seems like a viable way to mitigate the difficulties associated with the presentation and verification of IDs.

A digital ID is defined as all personal information that can be used in the presentation and verification of a person's identification and be collected, stored and verified electronically.[2][3]

[1] BKM ve Accenture Dijital ID Report, 2018

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

[3] G20 DIGITAL IDENTITY ONBOARDING, 2018. World Bank Group.

A digital ID service is a solution used for ID presentation and verification while a Digital ID System comprises all the components that allow the service to work.

2.1. Areas of use for digital IDs and digital ID ecosystems [1] [2]

The following are examples of common services with a need for identification where digital IDs can provide the aforementioned benefits.

The required ID data and a recommended list of stakeholders have also been identified for the use cases.

(*) In the first stage, the following 12 ecosystems (Table 1) and 71 use scenarios related to these ecosystems have been created. With the concept of ecosystem; is the structure consisting of real and legal stakeholders in a certain area and the interactions between them.

Table 1. **Ecosystems suitable to digital IDs**

FINANCIAL SERVICES	RETAIL (ONLINE AND IN-STORE)
FİNANSAL HİZMETLER	HOUSEHOLDS AND SHELTERS
HEALTHCARE	MOBILITY
EDUCATION	CULTURE AND ENTERTAINMENT
COMMUNICATIONS	BUSINESS / TRADE
TRANSPORTATION AND ACCOMMODATION	INSURANCE

[1] https://www.mckinsey.com/industries/financial-services/our-insights/remaking-the-bank-for-an-ecosystem-world

[2] Digital Identity Workshop Report of May 2018, which was created after the workshop, which was provided by Fjord and was held with the participation of BKM and 9 banks.

3. THE STAKEHOLDERS IN THE ECOSYSTEM

As can be seen in the use cases, digital IDs come with a multi-stakeholder ecosystem. The stakeholders in the ecosystem can take on different roles based on the information they have, the information they need and their respective competencies. A stakeholder's role can change and the same stakeholder can take on multiple roles at the same time.

Five levels of stakeholder roles have been identified based on the use cases in the previous section. The first three roles each correspond to a use case. As mentioned earlier, the same stakeholder can take on multiple roles at the same time.

The following are five different roles that a stakeholder can take on, with an example of a stakeholder for each role for a real estate loan application use case.

Role Level 1

Information-verifier

- Stakeholders with highly-trustable sources of identification information
- Approves/guarantees the veracity of the digital information
- Can be from the public sector or the private sector

Stakeholder example: Turkish Revenue Administration

Role Level2

Information-enricher

- Provides trustworthy information that can be added to the user's profile

Stakeholder Example: An expert network firm / A specialist company

Role Level 3

Information-user

- Needs / uses the identification information
- Requests digital information from the user to provide services to the user
- Safely stores the information upon the authority granted by the user

Stakeholder Example: Turkish Revenue Administration

Role Level 4

Information-owner (The person concerned)

- Is a natural person
- Needs their digital documents verified or personal information presented in order to gain access to a service

Stakeholder Example: Loan Applicant

Role Level5

Managers and Auditors

- Keeps the system up-to-date based on changing requirements
- Checks that the system functions the way it was designed to
- Undertakes other tasks such as the inspection of records

Stakeholder Example: Banking Regulation and Supervision Agency

3.1. Ecosystem Use Cases

The use cases and stakeholders of 12 different ecosystems have been listed in Table 2 and Table 3. Details on the use cases can be found in Appendix – 1.

Due to the overlap between different ecosystems, one use case can fall under more than one ecosystem. Yet, in the following examples, each use case has been matched with a single ecosystem to avoid repetition.

Table 2. Use Case Examples

PUBLIC SERVICES	• Applying for a driving license • Starting court proceedings • Obtaining a birth certificate • Transferring land • Obtaining a marriage certificate • Obtaining a sports license • Signing on to e-government • Giving the power of attorney • Applying for a job / an internship • Paying taxes / fines
FINANCIAL SERVICES	• Opening a personal account • Opening a commercial account • Becoming an online-banking / mobile-banking customer • Applying for a loan product (loan, credit card, etc) • Cashing / writing an e-check • Notifying somebody about a SIM card change • Sharing personal / verified information obtained from a bank • Buying / selling investment products • Buying / selling crypto assets • Performing transactions at financial institutions other than banks
HEALTHCARE	• Creating an e-prescription • Obtaining a statement of health from a doctor/physician • Obtaining an unfit for work note • Getting examined at a health care provider • Getting drugs / prescriptions at a pharmacy • Obtaining lab results • Obtaining mandatory provisions as part of a health insurance • Visiting a hospital • Accessing health information / healthcare as a refugee using digital IDs • Accessing health information / healthcare as an immigrant using digital IDs
EDUCATION	• Obtaining a diploma • Obtaining a transcript • Registering at a school • Transferring to another educational institution • Registering at a dorm • Identifying Turkish University Entrance Exam (OSYM Exam) takers through a biometric verification of their physical features • Accessing education information as an immigrant using digital IDs • Accessing education information as a refugee using digital IDs • Applying to the Higher Education Student Loan and Housing Board of Turkey

COMMUNICATIONS	• Subscriptions (sign-up, transfer, cancellation etc.) • Registering an e-signature
TRANSPORTATION & ACCOMMODATION	• Booking a hotel / checking in • Buying tickets and checking in at the airport • Renting items such as cars, drones and bicycles • Applying for a visa
RETAIL (ONLINE AND IN-STORE)	• Shopping online or in-store • Loyalty Programmes (cashing earned benefits or earning benefits) • Reciprocal credibility checks in international trade (the verification of financial information) • Selling regulated products (i.e. guns, alcohol, etc.) • Using Captchas
HOUSING / SHELTERS	• Signing up for compulsory earthquake insurance • Renting apartments • Utilities (electricity, water, etc) • Moving and renovations
MOBILITY	• Signing up for compulsory vehicle insurance • Using local transportation platforms such as Uber, taxis and Scotty • Signing for somebody else's cargo / delivery • Using shared transportation-services (automobiles, buses) • Car maintenance and repair
CULTURE, ENTERTAINMENT AND ADMISSIONS	• Buying tickets / loyalty cards for events • Age verification at events • Lotteries / games of chance • Entering buildings / office blocks • Entering common areas such as gyms • Entrustment items (e.g. headphones in a museum, headphones used in translations)
BUSINESS / TRADE	• Selling motor vehicles • Customs brokerage • Smart contracts used in the purchase and sales of goods • Starting a business • Selling precious metals
INSURANCE	• Applying for an insurance[1] • Making an insurance claim

[1] Under the insurance ecosystem, general insurance applications are specified and the Compulsory Earthquake and Traffic Insurance usage scenarios are listed under the Home / Housing and Mobil Mobility ecosystems respectively.

3.2. A recommended list of stakeholders for the digital ID ecosystem

Table 3. **List of stakeholders**

PUBLIC SECTOR STAKEHOLDERS

- Banks
- Banking Regulation and Supervision Agency
- Social Security Institution
- Hospitals
- General Directorate of Civil Registration and Nationality
- Ministry of National Education
- Institutes of Education / Schools
- Turkish Revenue Administration
- Turkish Ministry of Justice
- Ministry of Customs and Trade
- Ministry of Health
- General Directorate of Land Registry
- Municipalities
- Ministry of Youth and Sports
- Notaries
- Utility Companies
- The Financial Crimes Investigation Board
- The Union of Chambers and Commodity Exchanges of Turkey
- The Central Civil Registration System
- Central Bank of the Republic of Turkey
- Consulates
- Capital Markets Board of Turkey
- The Identity Information Sharing System
- Council of Higher Education
- Yurtkur
- Measuring, Selection and Placement Center
- The Disaster and Emergency Management Presidency of Turkey
- Museums
- Turkish Catastrophe Insurance Pool

PRIVATE SECTOR STAKEHOLDERS

- Banks
- Hospitals, healthcare institutions and doctors
- Insurance firms
- Pharmacies
- Investment / asset management companies
- Intermediaries
- Factoring / Leasing / Consumer-financing / Payments companies
- Driving courses
- Realtors
- Hotels / Tourism companies
- Charities
- Sports institutions / clubs
- Organizers of sports events
- Institutes of education / Schools
- Utilities companies
- Expert network firms / Specialist companies
- Automobile companies / car dealerships
- The Turkish Credit Bureau
- Takasbank
- Interbank Card Center
- Borsa Istanbul
- Mobile phone / telecommunications companies and internet providers
- Ticket offices, transportation / accommodation / tourism companies
- Car rental platforms / companies
- Courier delivery services companies
- Vehicle inspection, maintenance and repair companies
- Renovation services companies and marketplaces
- Museums
- Ticket office companies / platforms
- Jewellers
- Trade chambers

4. THE FUNDAMENTAL DESIGN PRINCIPLES OF DIGITAL IDS

12 fundamental principles are recommended for the design of digital ID verification services.

4.1. Privacy-focus

›› The specifics of the identification information and the duration for which it is shared are determined by the user

›› Access to the identification information belonging to the user is limited to the user and entities authorized by Law

›› Must be possible to hide parts of the identification information as needed, even from those with access to the rest of the information

›› The digital ID owner must be allowed to keep their information private, unless otherwise required by the Law

›› The digital ID owner must be free to share their information with institutions / organisations and / or grant access to the information for a specified duration / indefinitely. In cases of indefinite access or access with a specified duration, the system must make sure that the institution with whom the information is shared cannot permanently store the information on its own system

›› The ID information must be used only in the transaction for which it was intended; measures must be put in place to ensure that different pieces of information on the same user gained through different transactions are not associated with each other

›› There must be measures in place to prevent the unnecessary or erroneous disclosure of information

›› Identification information must be requested and processed as part of a transaction, in line with the purpose of the transaction and in proportion to the needs of the transaction

›› The information shared must be the minimum amount of information necessary to satisfy an information request

›› The services must comply first and foremost with Turkish Personal Data Protection Law No 6698 and its amendments, the Personal Data Protection Authority's guidelines and its Committee's resolution and any other local or international laws

4.2. Safety

›› Only information verified by the relevant institutions is used. However, if the institution requesting the information doesn't require verified information, unverified information can be shared

›› Must be robust to cyber-attacks. It must have the capability to monitor cyber-attacks. Security systems and teams must be in place to immediately mitigate any attacks

›› Orientation standards must be prepared to safely incorporate any new institutions and organizations who want to join the digital ID system as stakeholders

›› The ID system must have measures in place to prevent the ID information from being read, edited/deleted without permission or stolen. Users should not be able to make any unauthorized changes.

4.3. Accessibility and Portability

›› The system must not be dependent on any hardware or operating system

›› The system must be universal and accessible by a large audience

›› The digital ID data must not be stored in a central system or device; indefinite / limited mobile access to the data must be granted to the information-requesting institution

›› Must comply with local and international standards

›› Must be portable and accessible from any location

4.4. User-Centricity

›› The system shouldn't be service- or provider-centric, it should be user-centric

›› The user must be able to manage how their identification information is shared

›› The user must be able to choose which provider to use for their identification verification

›› The digital ID owner must be able to share their identification information with the institutions / organizations of their own choosing. The user must also be free to grant or limit data access.

4.5. Transparency

›› Whenever any information is shared, the information-owner must know the purpose for sharing and the duration for which the information is shared

4.6. Scalability

›› The system's performance must be unaffected from an increase in the number of stakeholders and transactions on the system

4.7. Performance

›› Connection speeds should not affect stakeholders negatively

›› The system must have a governance structure in place to update the system based on new requirements / standards and to track system performance

4.8. Usability

›› Must be simple and easily understandable

›› Must need minimal user intervention

4.9. Openness to collaboration

» Must comply with international standards; must be possible to collaborate with international ecosystem stakeholders if needed

» IDs should be usable across ID management systems and other relevant systems

» Must have the required infrastructure in place to allow different institutions to easily integrate into the system

4.10. Auditability

» Transaction authorizations must be trackable

» Must not allow information to be edited without leaving a trace

» Information records must be safely stored and be auditable

4.11. Flexibility

» As technology progresses, the system might need to be updated. The procedures needed to update the system must already be identified

4.12. Permanence / Durability

» Must be designed to be resilient to social, economic, political (e.g. war) and natural (e.g. disasters) circumstances

5. ID MANAGEMENT MODELS

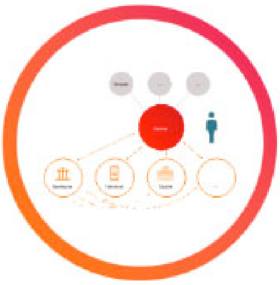
There are four types of service architecture to manage digital IDs.

» **Central:** Data is owned and controlled centrally; all stakeholders in the system feed their data into a central database and use the data from the same central database

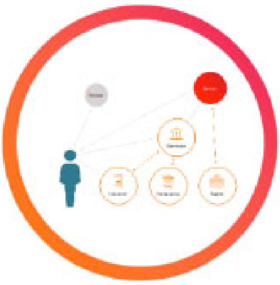
» **Federated:** Data is owned and controlled by certain stakeholders in the ecosystem, yet the final authority is a separate central authority

» **Distributed**: Data ownership and control are managed by the user; the stakeholders in the ecosystem can use / share the data with the user's permission

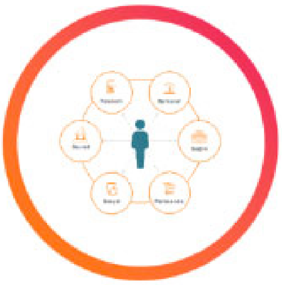
Central



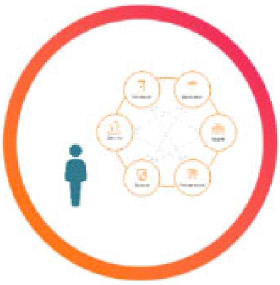
Federated



Distributed



User-centric



>> **User-centric:** Data ownership and control completely belong to the user; the stakeholders in the ecosystem don't have any data on the user.

Models other than these four are expected to become outdated.

Keeping the data centrally or tied to a central authority (as in the federated model) conflict the design principles of privacy, transparency, laid out in the fourth section. On the other hand, information is stored in its place of origin, in line with its purpose of creation and any business and legal regulations. For example, healthcare information is kept by healthcare institutions, educational information is kept by educational institutions and financial information is kept by financial institutions. Yet, as can be seen in the use cases, there is usually more than one place where an attribute of an ID is created and used.

This report discusses the distributed and user-centric models of service architecture as they comply with the design principles laid out in section four and are widely used around the world.

	Decentralized model << I have a verifiable ID>>	**User-dominant model** << I am whoever I say I am >>
DATA OWNERSHIP	• Identification information is fully controlled by the user • Stakeholders in the ecosystem use and share the information with the user's permission • Different stakeholders possess different parts of the identification information but a single stakeholder doesn't have all the information • The user's consent and interoperability are essential • The identification information is stored in its place of origin and is verified upon user request but does not change hands	• Identification information is fully controlled by the user • The stakeholders in the ecosystem don't have any data on the user • The user is the only authority on the identification / personal data and the data's usage • The user's explicit consent is the basis; the user is the owner of the ID and has the right to create and delete IDs
ID	• The user can create / store their ID using different providers • The user can share their identification information with persons and institutions of their own choosing • This model is an updated version of user-centric model; unlike the user-centric model, it allows the user to control with whom and how the identification information is shared, can be managed from a single point and has interoperable IDs	• The ID's portability is the basis; the system is not dependent on any provider or data store • The user can be their own ID-provider • More than one verifiable ID claim can be made for the same user (by the user or another publisher) • Every service provider is free to decide which publishers' IDs to trust

6. A TECHNOLOGICAL ASSESSMENT OF DIGITAL ID MANAGEMENT SOLUTIONS

6.1. Central / Distributed Technologies

Choosing the right personal data management model is critical to ensure that digital ID services are universal, uninterrupted and of high accuracy. As can be seen in the table below, there are different advantages and disadvantages to keeping the data centrally or distributed.

Even though it is easier to keep data in a central model up-to-date, data in a central model must be protected against any unwarranted changes. Additionally, it is difficult to keep a central system accessible in unexpected circumstances or in the event of an attack.

On the other hand, keeping data up-to-date in a distributed model can be difficult. Yet, it is much harder to edit the data without the proper authorization in a distributed model.

Distributing the data across the system can also make access to the data easier. On the other hand, it is difficult to prevent data stored in different places from surfacing.

Table 4. **Comparison of Central and Decentralized Systems**

	Central Technologies	Distributed Technologies
Advantages	• Easier to manage • Easier to create mechanisms which prevent personal data from surfacing	• The distributed structure of the data reduces the risk of unauthorized changes • Easier to ensure accessibility since information can be accessed from multiple sources
Disadvantages	• Require more protection to guard against unwarranted data changes • More expensive to keep the system accessible and prevent it from being a single point of failure • Requires further protection against internal threats	• Additional mechanisms are needed to ensure that data in different locations are up-to-date and consistent • More difficult to prevent personal data from surfacing

7. “BLOCKCHAIN” IN DIGITAL ID SOLUTIONS

Blockchain is one way of implementing distributed ledger technology. Records / transactions are stored distributed using a reconciliation mechanism. Therefore, all records can be kept distributed instead of centrally, which would require high security measures. The cryptographic mechanisms used allow the transaction records to be linked to each other in chains, allowing the transactions to be irrevocably and unalterably recorded.

Distributed systems and databases have been in use for a long time. What’s different with blockchain is the trust in the veracity of the data stored in the blockchain.

Considering its advantages, blockchain seems to be a suitable building block on which to develop digital ID systems.

The protection of personal is data is becoming more important both globally and in Turkey. Under current laws and regulations, clear consent from the person is needed to collect personal data. Additionally, personal data has to deleted if the person to whom the data belongs wants it to be deleted. Therefore, blockchain can be used to store the data’s authenticity and access proofs, instead of original copies of the data.

In order to prevent unauthorized access to the data, part of the data can be stored on blockchain while the rest of it is stored on systems outside of blockchain and / or only the proofs, summaries or encrypted versions of the data can be stored on blockchain.

On the other hand, blockchain is still a technology-in-progress. The development of scalable and safe reconciliation mechanisms is crucial for the usability of blockchain. If an internationally acceptable solution is developed, an internationally acceptable system can be built.

8. OPEN AREAS

The following topics need to be clarified in order to make the digital ID system usable and widespread. These topics have been grouped under six areas and detailed. For further assessment, critical questions, issues that need to be solved and suggestions have been identified. The following are meant as a guideline and do not cover all the required next steps.

1.Technical Model: Choosing a model that complies with the fundamental principles

2. Governance and working model: Setting up a working model covering and protecting all stakeholders

3. Standards: Complying with standards

4. Legal considerations and regulations: Complying with the relevant legislations

5. Safety and privacy: Implementing usable security and privacy by design

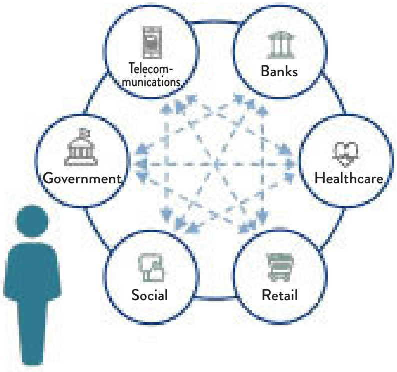
6. Determining the digital ID work flow and lifecycle: Keeping the system simple and understandable to ensure ease of use

8.1. Technical Model[1]

Management model of the ID verification system can be central, federated, distributed or self-sovereign. A privacy focus has led self-sovereign digital id systems to become popular around the world. The service architecture must be chosen to fit the desired design principles.

The advantages and disadvantages laid out in Table 4 must be taken into consideration when choosing a model. The model will affect where and how records will be kept in the system and how they will be shared.

Modern-day systems must be agile to satisfy fast-changing needs. Thus, the system must be agile to adapt to the quickly changing needs. To evaluate these needs in question from technical and administrative perspective and put them into effect, a governance mechanism should be constructed.



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

8.2. Governance and Working Model[1]

Setting up an effective and efficient multi-stakeholder digital ID system requires bringing stakeholders from different sectors together. These stakeholders have to determine which decision mechanisms to put in place and how these mechanisms should work in order to answer questions on the amount and type of investment to be made, rules of operation and technical standards. Setting up and operating such a system requires investment. Institutions willing to make the necessary investment must be identified, a governance structure must be set up and a business plan must be formed. Furthermore, the data needs to be of high quality to ensure the venture's sustainability and the ID service's trustworthiness. In order to make the data to be of high quality the stakeholders must be able to generate commercial income.

The following principles are suggested for setting up the governance and business model:

1.It would be useful to have a setup in which institutions have access to up-to-date information on the digital ID system for all of their services.

2. Keeping an inventory of the least amount of information that needs to be requested for a specific service, an authorization mechanism to limit the level of information in verification processes and a list of providers with up-to-date information would be useful.

3. Users must be able to control the information they would like to share using a dashboard. Additionally, unauthorized access to information that the user would like to keep private should be prevented.

4. A monetization method must be identified to operate the system and make the system valuable for all stakeholders. In a monetized model, institutions and organizations verifying the information and organisations running the system would be allowed to charge a fee. A feasibility study to identify a suitable revenue model would be useful.

5. A governance model authorized to determine which updates to carry out based on evolving needs must be put in place.

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

8.3. Standards

The new system must be able to operate on an international scale. Thus, it must comply with national and international standards. For example, European Union's e-signature and identification verification standards must be taken into consideration.

Area	Topic	Decision Areas
Public Key Infrastructure (PKI)	The public key infrastructure to be used in the system should be determined.	1. Central PKI[2] / Non-Central PKI[3] 2. Who holds the authority of certification, how should they be authorized 3. Providing time-stamps[2][4] 4. Approving-/verifying- organizations 5. Ensuring the security of private keys
Verifiable Credentials	Attributes and format of the digital ID should be determined.	1. A unique identifier for every relationship type 2. Decentralized identifiers (DID)[5] for every relationship type (only the person and authorized organizations can determine who owns the identifiers / assign identifiers) 3. The resolution mechanism of the digital information owner (public key etc.) from identifier 4. Updating the information 5. Revocation mechanisms
	The approval and verification mechanisms of verifiable credentials should be determined.	1. Central models • The creation verifiable credentials is limited to publishing / verifying institutions 2. Distributed models • The creation can be undertaken by the user (assertion) • The publishing / verifying institution attests for the credentials (attestation) 3. The credential is verified using the signature appended to it and/or using data from the blockchain. If needed, a trustworthy institution is asked to validate the information (validation) 4. The joint use of central and distributed models
	A mechanism to find authorized institutions to be used in gathering and verifying digital information/documents should be put in place.	1. A service catalogue (naming & discovery) 2. Authorization mechanisms
	The ownership of digital IDs and verifiable credentials must be determined.	1. They are belong to the user 2. They are belong to authorized public institutions 3. They are belong to their verifier 4. They are belong to the service provider
	The verifiable credentials should have an expiry date.	1. Stable information (certificate of birth, diploma, etc.) • An expiry date is not required • Should be possible to revoke the documents if needed 2. Unstable information • An expiry date should be set • Should be possible to revoke the documents before the expiry date if needed
	It should be possible to associate verifiable credentials with the subject.	1. Only the information owner can associate the documents with the subject 2. Authorized institutions can associate the documents with the subject

Area	Topic	Decision Areas
Verifiable Credentials	Safe storage mechanisms should be identified to store the verifiable credentials.	1. The informationstored solely on the information-owner's devices (verifiable credentials, private keys etc.) 2. The information stored in service-providing institutions 3. The information stored on blockchain 4. The information stored in publishing / verifying institutions
	The acquisition method of verifiable credentials should be determined.	1. Explicit consent management 2. Where to acquire the verifiable credentials 3. What kind of information is needed 4. How long the verifiable credential is valid for 5. Who initiates the process • The user starts the process • The service provider starts the process • The authorized institution starts the process
	The transmission method should be determined.	1. Transferring the verifiable credential from the owner to the service provider 2. Transferring the verifiable credential via the approving / verifying institution 3. Transferring information on transactions to be written on blockchain
	The verification method of credentials must be determined.	1. The service provider can verify the credentials using the data on blockchain • If the verifiable credential is valid, it can be used more than once 2. The publishing institutions can verify the information / documents • The publishing institution must be contacted for each verification
Registration	Registration centers must be identified.	1. Public institutions 2. Turkish Post Office (PTT) 3. Banks 4. Telecommunications providers
	Entry points to the system should be determined.	1. Stable information (certificate of birth, diploma, etc.) • An expiry date is not required • Must be possible to annul the documents if needed 2. Unstable information • An expiry date must be set • Must be possible to annul the documents before the expiry date if needed
	It must be possible to associate the digital documents with the subject, if needed.	The available services can be dependent on the type and method of entry. • E-government (password, ID card, e-signature, mobile-signature) • Banks (internet-banking) etc.
The blockchain model[1]	The blockchain model should be determined.	1. Public / Private (Permissionless / Permissioned) 2. Open access / closed access
Other	The main design principles laid out in section 4 of this document should be considered.	

[1] eIDAS Regulation (EU) No 910/2014

[2] Public Key İnfrastructure For Financial Services: https://www.iso.org/standard/63134.html

[3] Decentralized Key Management and DPKI: https://bit.ly/2RCavx5 https://bit.ly/1TEd4bB

[4] Time Stamping on Blockchain: https://chainpoint.org/

[5] W3C DID Specifications: https://w3c-ccg.github.io/did-spec/

[6] W3C Verifiable Claims WG: https://www.w3.org/2017/vc/WG/

[7] W3C Verifiable Credentials Data Model 1.0: https://w3c.github.io/vc-data-model/

[8] NIST-IR 8202: Blockchain Technology Overview, https://doi.org/10.6028/NIST.IR.8202

8.4. Legal Considerations and Regulations

As digitalization becomes more prevalent in our changing and developing world, it becomes necessary for the legal world to address it. As a branch of social sciences, law evolves as life evolves and law is currently trying to keep up with the new requirements brought on by digitalization. In other words, the current law/regulations are expected to change and/or expand to be able to cover new problems brought on or foreseen to be brought on by new developments. Current legislation is human-centric (which is in-line with the needs of our current world and lifestyle), covering humans, the actions of humans and their deeds. Yet, the current trend of digitalization predicts the exact opposite to prevail. The human factor that the current legislation covers is expected to give way to objects, inter-object communications, the objects' integration, artificial intelligence, robots controlled through software / hardware and smart factories that can operate without any manpower. Following this digitalization trends, the judicial system has already started working on understanding what needs to change and making changes.

The concept of "data" is at the centre of the global digitalization trend. Not only should the use and processing of this data should be protected under law but digital IDs, which are a form of data-based digitalization, should also be regulated.

8.4.1. The structure of regulations related to Digital IDs

Based on examples from global sources and Turkey, regulations covering digital IDs have the following hierarchical structure:

They are general laws, made by the legislative branch. They apply to all ID systems and ID system stakeholders by virtue of the authority vested by the government.

These laws do not directly regulate ID systems. Yet, due to their nature, they often include mechanisms that regulate ID management and ID systems and determine the authorities related to and rules on ID-related activities / transactions.

In 2018, digital IDs became more widespread and advanced. Digital driving licenses, mobile ID applications and digital passports are the leading examples of this phenomenon.

One of the most important regulations related to digital IDs is the regulation on e-signatures.

Even though there is not any specific regulation directly covering digital IDs in Turkey, the foundations were laid through Law No 5070 on electronic signatures ("The e-signature law"), which came into force on 23rd of July 2004. The e-signature law differentiates between a safe e-signature and a regular e-signature, defines what timestamps, digital data and digital certificates are and covers relevant regulations. Following the e-signature law, the legal foundations for a regulation on mobile e-signatures were laid out in the decree on electronic signatures, e-signature processes and technical criteria[*].

[*] Communique on electronic signature processes and technical criteria

Other regulations that can be applied to digital ID systems include the Turkish Civil Code (No 4721), the Civil Registration Services Law (No 5490), the passport law (No 5682) and the Turkish Citizenship Law (No 5901).

In addition to the aforementioned regulations, the protection and privacy of personal data should form the basis of any digital ID system. The protection of personal data in Turkey is regulated by the Turkish Personal Data Protection Law (No 6698) and any secondary amendments.

Digital ID systems have risk by nature: They can be used as tools of surveillance. The system inevitably gathers sensitive information such as a user's location, when they were at the location, the types of information the user uses and how many times a certain ID has been used. This type of information directly impinges on a user's private sphere. If we are to move to a completely digital economy, strong data protection laws need to be put in place to ensure that the collection, storage and sharing of personal attributes, which are collected during identification registration in a country, are done in a safe and suitable manner.

8.5. Safety and Privacy

Cases of personal data theft have become more prevalent in recent years. One reason is the increase in the use of online services such as e-government, e-municipality, internet banking and online retail as internet use becomes more prevalent. Another reason is the limited amount of security measures in these online services. However, the real reason of personal data breaches is the lack of a focus on the privacy protection in the design phase (privacy by designs) of these services and systems. Thus, new standards with a privacy-focus, such as ISO 27018 and ISO 29100 have been created, despite the existence of general standards of safety, such as ISO 27001.

Digital ID systems make storing, processing and sharing big data technically possible. In the process, sensitive personal information related to education, healthcare, finance, location and time will be processed. These systems are attractive for hackers due to the sensitive nature of the information they contain. However these systems should not be prone to data breaches and must not become single points of failure, potentially causing services to stop. In this context, the tetralogy of privacy, confidentiality, integrity, availability, as well as cyber security, is fundamental and must be taken into consideration in the application of digital ID systems. User confidentiality, which includes the protection of user data and personal data, must be maintained in line with current legislature (GDPR and KVKK).

Cyber attacks are becoming more prevalent day-by-day. Attackers are using highly destructive/lucrative strategies such as virus/trojans, ransomware or denial of

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

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

[3] ISO Standard: Information technology, security techniques, privacy framework

service attacks to target intellectual property, personal data, health records or financial data. Both citizens and institutions are affected by these attacks as not only is sensitive information compromised but also operations are suspended. Therefore, when a digital ID system is built, strategies and technical measures to minimize the repercussions of a cyber-attack must be used.

Due to its nature, blockchain technology does not have a single point of failure, which makes uninterrupted access more likely. This feature also largely decreases the repercussions from denial of service attacks. Blockchain minimizes fraudulent behaviour due to its consensus usage.

Data written on blockchain cannot be changed due to its cryptographic mechanisms, which increases trust in the data in the blockchain. Blockchain technology can greatly contribute to the development of cyber-protection in digital ID systems. Yet, cyber risks on the user side still persist, such as in situations where applications such as Client/Wallet are used.

8.6. Determining the digital ID work flow and the lifecycle

The fundamental design principles laid out in section four must be considered when creating the workflow and lifecycle of digital ID system. Some questions that need to be answered in this context are as follows:

›› Should biometric features (which are harder to change by their nature) be used for digital IDs? (e.g. for accessing keys stored in mobile phones or safety devices)

›› Mobile phone number

- Should it be a part of the digital ID?
- Should it be a requirement?

›› In cases where the Know Your Customer (KYC) process is undertaken by a bank:

›› Can a user use the services of a bank without becoming its customer?

- Can foreign currency be bought/sold at another bank's exchange rate?
- Other relevant transactions can be identified (every product / service might not be technically feasible)

›› Cases of forgotten, unusable or compromised (such as when they fall into unauthorized persons' hands) login / access information for the digital ID system must be handled in the lifecycle or key management

- How will re-entry into the system work?
- Is it possible to make back-up and recovery mechanisms simple, fast and durable against fraud?

›› Can back-up ownership, protection and modifiability be addressed without putting personal information at risk?

›› Taking precautions against the dispersion of a fraudulent account, which has wrongfully but successfully passed the Know Your Customer (KYC) stage?

9. GLOBAL DIGITAL ID EXAMPLES

In the near future, the up-and-coming technology blockchain is expected to change the ways of doing business in many sectors and has many different areas of application.

Smart contracts, where the details of the contract can be automatically controlled, splitting an asset through digital tokenization, improving supply chains by recording manufacturing parts and processes digitally and ensuring the security of IoT platforms through blockchain are only a handful of the different applications of blockchain technology.

Digital IDs, which are a product of the fundamental and global need for IDs, are amongst the most important areas of blockchain application.

uPort, New York, USA

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

- Comprises of three main components: Smart contracts, developer libraries and mobile applications
- IDs are self-sovereign, meaning the content-owner has full ownership and control and doesn't rely on a central authority / third party for creation or approvals
- Since the IDs are blockchain-based, they can be used to manage digital carrier items such as cryptocurrencies or other tokenized assets
- An Ethereum-based digital ID system

Verified.Me, Toronto, Canada[4]

https://verified.me/

- A blockchain-based digital platform, developed by SecureKey Technologies Inc.
- Allows the identification owners to safely verify the identification information online and provides mobile-access services and products
- Ecosystem stakeholders include Desjardins, The National Bank and The Big Five banks in Canada
- A hyperledge-based digital ID system

CIVIC, San Francisco, USA

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

- Allows users to control their identification information; uses blockchain ID-verification technology to ensure safe sharing of personal data
- Aims for password-free authentication by relying on the blockchain and biometric technologies on phones and its non-central architecture
- The future roadmap of the platform includes building an infrastructure for international KYC verification
- An-Ethereum based digital ID system

AADHAAR, India[1]

https://uidai.gov.in/

- Is a biometric ID platform that stores citizens' biometric (iris and fingerprints) and demographic information; it is managed by the legal authority UIDAI
- Digital ID information is stored on blockchain architecture using the national identity number (the Aadhar number)
- Every transaction by every user is keyed and private keys created as a result of transactions are destroyed
- A private Blockchain-based digital ID system

IDHub, Beijing, China

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

- Takes advantage of smart contracts and non-central blockchain technology; grants its users id-control/dominance
- Its design principles are dominance, safety and privacy
- The stability of the blockchain architecture and the NaCl library is ensured through Kademlia, a distributed storing platform
- A private Blockchain-based system

ID2020, International[2] https://id2020.org/

- Is a public sector and private sector partnership, dedicated to improving life through digital IDs
- Brings international non-profit institutions, for-profit institutions and governments together to identify the technical standards for a safe, user-owned and user-controlled digital ID. Also finances pilot projects which provide digital IDs for vulnerable populations
- An Ethereum-based digital ID system

Sovrin, International[3] https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

- A new standard, designed to convert analogous IDs into Digital IDs
- Aims to give people and institutions the freedom to collect and carry verifiable digital IDs throughout their lives
- Through the concept of self-sovereignty, the individual digital ID owner is allowed to access and use their identification information on the system whenever they want
- An open and authorization-based digital ID system

[1] https://www.emudhra.com/case-studies/Whitepaper_Blockchain.pdf
https://www.mygov.in/frontendgeneral/pdf/white-paper-mobile-as-digital-identity-v0-2.pdf

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

[3] https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

[4] https://2m6dvv3zi6nj31h9a91s1wdk-wpengine.netdna-ssl.com/wp-content/uploads/2018/05/Case-Study-government-of-canada.pdf
https://securekey.com/digital-id-ecosystem/

CONCLUSION

In the modern age of fast technological change, digital IDs provide great value for people and institutions. According to a McKinsey report, digital IDs can create cost savings of up to 90% and allow more people to join the financial system.

Digital IDs are personal, managed by the ID-owner, accessible at any time and from any location, permanent and universal.

Based on successful global examples, design principles and ID-management models, the use of distributed models of collaboration to manage digital ID services is inevitable in order to ensure a sustainable digital ID project. It is our greatest hope that the collective method of working seen in Turkey in other sectors be implemented in the digital ID space and allow us to move towards a more digital Turkey.

[1] MGI Digital Identification

GLOSSARY OF TERMS

- **Ecosystem:** Natural and legal persons in a specific field and the interactions that take place between them
- **Use case:** An example of digital ID application; includes relevant stakeholders and the relationships between the stakeholders
- **Issuer:** The creator of the information
- **Public Key Infrastructure:** The infrastructure used for managing keys used as e-signatures throughout their lifecycle (i.e. creating a key, deleting a key etc.). Can have a central, hierarchical or distributed model.
- **Key Management:** The mechanism with which all the keys in the system are managed. Can be central or distributed.
- **Timestamp:** Proves that the digital information existed before a certain date. Can be provided by the certificate authority or through blockchain.
- **Unique Identifier:** Allows the persons in the system to be uniquely identified. The Turkish identification number is an example. Public keys or their summaries can be used.
- **Verifiable claims / credentials:** Is created by the W3C verifiable claims working group. Comprises the set of data that can be verified by institutions authorized to provide information about the person, can provide cryptographically-strong security, ensure privacy and be verified by the machine.
- **Near-field communications:** A technology that allows small amounts of data transfer between two devices which are a few centimetres-apart.
- **W3C:** World Wide Web Consortium
- **KVKK:** Turkish Personal Data Protection Law
- **GDPR:** European Union General Data Protection Regulation

CONTRIBUTORS

Demet Memiş
Accenture

Mehmet Albayrak
Murat Bitirici
Akbank

Mustafa Saraç
Albaraka Türk Katılım Bankası

İsmail Özeren
Anadolu Sigorta

Emek Akbak
Avivasa

Celal Cündoğlu
Özge Çelik
Bankalararası Kart Merkezi A.Ş.

Emel Özgümüş
Deloitte

Şahika Mut
Can Orhun
E-güven

Ufuk Özkan
Elif Ülger Göktaş
Ford Otomotiv Sanayi AŞ

Itır Ürünay Aydoğan
Efe Kaşoğlu
Arda Çolak
Garanti Bankası

Fırat Dürüst
Tolga Gümüş
Halim Memiş
Boğaç Devrimci
İş Bankası

Erman Taylan
Koç Finans

Gökhan Murtezaoğlu
Koç Sistem

Merve Can Kuş
Hasan Özkul
Kuveyt Türk

Seda Akdemir
Ferhat Dilman
Duygu Ateş
Microsoft

Dr. Att. Çiğdem Ayözger Öngün
Att. Begüm Ertürk
SRP-Legal - Dr. Att. Çiğdem Ayözger Öngün Law Office

Darço Akkaranfil
İbrahim Kara
Umut Esen
Didem Gökçe Güçkıran
Softtech

Att. Çağhan Tansel
TANSEL Danışmanlık & Hukuk

Erdal Çokol
TEB

Gürcan Erim
Turkcell

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

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

Esat Belhan
Umut Keçecioğlu
Yapı Kredi Bankası

BLOCKCHAIN

TÜRKİYE

TBV

TÜRKİYE BİLİŞİM VAKFI