

Decentralized ID Checklist for US Healthcare

Companion Guide – Textual Reference Manual

University of St. Gallen | Columbia Business School

© Sophia Maite Magdalena Goeppinger

sophia.goeppinger@student.unisg.ch | sgoeppinger23@gsb.columbia.edu

Executive Summary

The Problem

The US healthcare system is awash in a sea of data. To ensure efficient operation of the healthcare system, the vast amount of data generated every second – from clinical and reimbursement data to product information – must be easily accessible, editable, and trustworthy. However, current data flows are disrupted, including malicious attacks, preventing this from being fully achieved.

The Cause

The primary culprits of disrupted data flows are conflicting interests and incentives among healthcare stakeholders and the lack of digitization of trustworthiness to transmit it across all types of communication channels between interacting stakeholders.

The Solution

Conflicting interests and incentives are predominantly driven by the pursuit of financial gains and other organizational self-interests rather than technical complexities. Conversely, the cardinal problem of easily transmitting trustworthiness across distance can be deciphered technically with decentralized identity (ID). Decentralized ID has particularly begun to garner attention as a bulwark in the forthcoming generative AI era.

The Point of the Decentralized ID Checklist

- ▶ **Healthcare has a track record of failures in health information system (IS) deployments:** Health ISs are touted as solutions to some of healthcare’s most pressing issues, but a significant percentage of such deployments fail.
- ▶ **Increase the likelihood of success:** The framework is intended to assist in evaluating whether a healthcare use case is amenable to decentralized ID before proceeding with any investments. This enables you to make informed decisions when selecting use cases for decentralized ID and planning corresponding initiatives.
- ▶ **Evidence-based framework:** The framework has been developed from theory and extensive primary research.

Initial framework applicability test: A precursor to the full assessment

This is a preliminary test to gauge if the framework suits your organization’s specific use case. A single “yes” justifies a more thorough exploration of the framework.

	Yes	No
You face identification, authentication, and/or authorization issues when interacting with external stakeholders.		
You face data quality issues when interacting with external stakeholders.		
You face security/compliance issues when interacting with external stakeholders.		

1 How to Use the Decentralized ID Checklist

- ▶ **Primary purpose:** The Decentralized ID Checklist aids US healthcare stakeholders facing digital trust challenges that require resolution and already have a specific use case in mind that decentralized ID may address in assessing whether a particular use case is appropriate for decentralized ID. In this context, it is crucial to note that the framework examines decentralized ID as a concept and does not concentrate on specific implementation solutions.
- ▶ **Domain-crossing framework design:** Decentralized ID is a multifaceted concept that extends beyond mere technology, encompassing legal, social, and business domains. The assessment model has been crafted using a domain-crossing approach to capture this multidisciplinary nature.
- ▶ **Within-organization target group:** The framework's design enables collaboration among different divisions in your organization, allowing each division to contribute its respective expertise. Upon completion, the assessment's results may guide discussions with your senior executives, followed by approaching external key healthcare stakeholders whose participation is required to address the use case.
- ▶ **Second-order uses of the framework:**
 - **Expectation management tool:** Deepens your understanding of decentralized ID and the underlying technologies as the driving forces behind this novel approach to ISs. By providing an overview of the capabilities and limitations of decentralized ID, it has the potential to deter opportunistic adopters from jumping on the bandwagon, hailing it as a panacea for every problem.
 - **Legitimacy provision:** Empowers your organization and managers to walk away from adopting a decentralized ID system before expending resources or devoting additional time to implementation planning.
 - **Implementation support tool:** Facilitates more informed decision-making in planning corresponding endeavors.
 - **Post-adoption project evaluation:** Facilitates explaining potential project failures retrospectively.
 - **Building block provision for context-specific needs:** While the framework has been developed based on the problems of the US healthcare system, its modular nature allows it to apply to other national healthcare systems and entirely different sectors with some smaller or larger modifications, depending on the sector.

2 Structure of the Framework

The Decentralized ID Checklist is divided into a preparatory stage and two tiers, the *critical amenability assessment* (Tier I) and the *comprehensive amenability assessment* (Tier II), which are defined by different amenability factors. Tier I evaluates whether applying decentralized ID for a certain use case is appropriate solely based on theoretical effectiveness. Tier II considers contextual and situational factors that are described by six dimensions, acknowledging that although a socio-technological innovation might seem promising in theory, practical challenges may emerge during its implementation (Flessa & Huebner, 2021). The division into two tiers offers an early assessment exit point. If Tier I yields negative results, it is not recommended to advance to the deeper use case

Before evaluating the two tiers, identify at least two individuals who work in the technology and commercial divisions of your organization, respectively. If a single individual or team rides the fence between these two divisions and can answer all the questions, that is wonderful. However, in many cases, it will be an information technology leader (hereby referred to as *Tech Division*) and a commercial leader with healthcare market knowledge (hereby referred to as *Commercial Division*). Have each leader and their teams complete their respective section, and you will have a comprehensive picture of whether your use case is amenable to decentralized ID.

Open the enclosed Excel workbook and begin drafting the use case in a clear and concise textual format. This will allow for the clear specification of any assumptions and facilitate the completion of the framework.

[illegible]

Use case: Facilitate Medication Prescriptions

Primary actor(s)/end-user(s): Physician, State Board of New York

Scope: Prescription process

Level: Summary (i.e., the entire prescription process is looked at)

Description: A board-certified physician practicing in New York writes daily prescriptions for his patients. To enhance accountability and verifiability in the prescription process, he desires a digital credential from the State Board of New York that confirms his certification to practice medicine in the state. The digital certificate enables attachment to the prescription, allowing the nearby pharmacy to verify his prescription writing privileges.

Tier I: Critical amenability assessment

Tier I assesses the appropriateness of decentralized ID to address the use case from a purpose-centric standpoint while omitting contextual factors.

With the drafted use case in hand, follow each step as indicated in the Excel workbook. Since Tier I begins with technical aspects, it is recommended that the Tech Division initiates Tier I. The Tech Division should start in the *Preparation* tab by determining if the use case involves healthcare stakeholders, which must provide you as an organization with some proof of trustworthiness, such as certifications or the Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement (BAA), to initiate an interaction with you. If this condition is met, proceed to identify whether there are any digital interaction issues involved in the use case. Here, only one of the four problem sections must be flagged as problematic to proceed with the assessment.

Upon completion of assessing the digital trust problems of the use case, hand the framework over to your commercial counterparts. The assessment requires them to list all healthcare stakeholders that would have to get involved for the use case to materialize, i.e., the *minimum viable ecosystem* (MVE). This is followed by the final step of the assessment framework, which involves analyzing whether all of these listed healthcare stakeholders have an incentive to address the digital trust problems of the use case. This last step determines if you should proceed to Tier II of the Decentralized ID Checklist for a more comprehensive evaluation by considering contextual factors.

Tier II: Comprehensive amenability assessment

Tier II, the comprehensive amenability assessment, evaluates the amenability of your use case to decentralized ID deployment through a weighted decision matrix that takes into account contextual factors. The assessment involves evaluating the alignment between 61 standardized decentralized ID amenability factors arranged in six use case dimensions and your use case’s characteristics. The suitability of decentralized ID solutions for the use case is determined based on this alignment. To conduct this evaluation, follow the steps outlined in the Excel workbook, as you did with Tier I. The screenecast may also be helpful in populating the assessment correctly since it provides a more practical and hands-on approach.

Critical Requirement Assessment (Tech Division)

Information

The words in *italic* are further specified in the User Guide.

Legend for requirement assessment model:
Please type in your comments/notes
Please use the drop-down menu
Tells you whether to proceed with the assessment or not

Critical requirement assessment framework

Step #	Instruction
Step 1	Have your decentralized identity use case in text form readily available for the asses
Step 2	Decentralized identity enables inclusive, trusted digital interactions. Does the use ca things) that need to be brought within the <i>trust boundary</i> in order to interact with y
Step 3	Assess whether you face at least one of the following problems when interacting wit

Output section >> Summary Detailed view of Tier II Input section >> Preparation Tier I (Tech division) Tier I (Com

Critical Requirement Assessment (Commercial Division)

Information

Your technical counterpart has already successfully concluded Step 1 to Step 3. Thus, they ask you now to proceed with Step 4, relying on
The words in *italic* are further specified in the User Guide.

Legend for requirement assessment model:
Please type in your comments/notes
Please use the drop-down menu
Tells you whether to proceed with the assessment or not

Your use case: Please type your use case in Cell B12 of the Tier I Use case tab

Critical requirement assessment framework

Step #	Instruction
Step 4	A decentralized identity's full potential can only be realized when all entities within the use case <i>minimum viable ecosy</i> involved entities that form the <i>MVE</i> and would have to collaborate for the use case to materialize and be addressed.
Step 5	Is there an incentive for every <i>MVE</i> stakeholder to address the digital trust problem(s)?

Output section >> Summary Detailed view of Tier II Input section >> Preparation Tier I (Tech division) Tier I (Commercial division)

To calculate the overall amenability score, both divisions are expected to follow these steps:

1. Assign a relative importance rating to each amenability factor from each of the six amenability dimensions (human, organizational, technological, systemic, collaborative, and wider macro-economic use case characteristics) based on your best judgment regarding its relevance to the use case's manifestation and handling. Begin by rating the first item (Column F) as "10" and then rate subsequent items accordingly. For instance, if an item holds the same level of importance, rate it as "10". However, if it's less significant, rate it as a lower number, such as a "7". On the other hand, if it's more crucial, rate it higher, such as a "40". The default rating for all statements is "10", giving you the flexibility to adjust its significance. Column G automatically displays the importance rating as a percentage.
2. Next, each amenability factor is evaluated on how well it corresponds to the particular use case. In Column H, go through the statements from top to bottom and rate each based on how well it aligns with your use case at hand (-2 = *strongly misaligns*, -1 = *somewhat misaligns*, 0 = *neutral*, 1 = *somewhat aligns*, 2 = *strongly aligns*). The rating scale assumes higher values indicate higher amenability of decentralized ID to the use case. Use Column I to record any important observations made while assessing each amenability factor.
3. It is important to anticipate potential changes to the importance level and rating of each amenability factor in the future. In Column J, indicate whether you expect any changes in the situation described for each amenability factor. If you anticipate any changes, use Column K to provide comments on how you believe these changes will occur.

Steps 1 to 3 are followed by both the Tech Division and Commercial Division in their respective Excel tabs, as indicated. Some managers may have concerns about quantifying such a subjective and qualitative process. Nevertheless, quantification of some form can aid in revealing and

C	D	E	F	G
Amenability factor keyword			Relative relevance rating	
Amenability factor			Relevance to your use case	(%)
1.1	Prior information technology experience	End-users and/or decentralized identity adoption decision-makers have a positive or neutral experience with information systems (including blockchain).	10	13%
1.2	Expected workload	The workload of the decentralized identity solution's end-users is not expected to increase.	10	13%

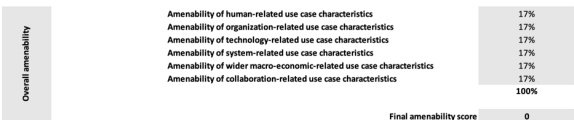
C	D	E	H
Amenability factor keyword			Alignment rating (2 to -2)
Amenability factor			Alignment with your use case
1.1	Prior information technology experience	End-users and/or decentralized identity adoption decision-makers have a positive or neutral experience with information systems (including blockchain).	
1.2	Expected workload	The workload of the decentralized identity solution's end-users is not expected to increase.	

C	D	E	F	G
Amenability factor keyword			Do you expect this situation to remain stable (i.e., NOT to change)? (Yes/No)	
Amenability factor			If you answered "No" to any amenability factor remaining stable, this provides you with space to make any comments to help us recall to use of implementation to come back to later on.	
1.1	Prior information technology experience	End-users and/or decentralized identity adoption decision-makers have a positive or neutral experience with information systems (including blockchain).		
1.2	Expected workload	The workload of the decentralized identity solution's end-users is not expected to increase.		

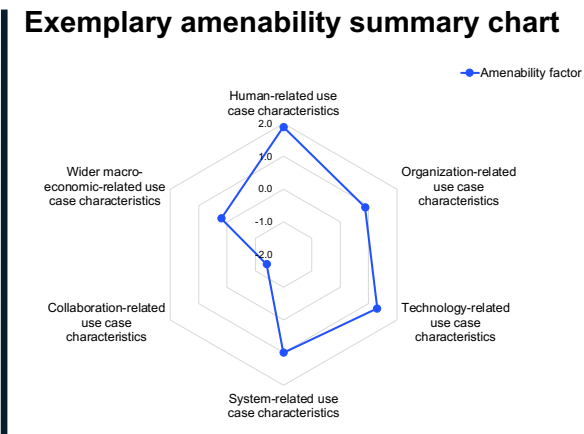
examining underlying assumptions regarding the implementation of decentralized ID, particularly in the early stages of such a potential undertaking (Cummings and Holmberg, 2012).

4. Finally, in the *Detailed view of Tier II* spreadsheet, both the Tech Division and Commercial Division jointly rate the amenability of each use case dimension according to its relative importance at the very bottom. This process is similar to the importance weighting of the individual amenability factors: Begin by assigning a relative importance rating of "10" to the *amenability of human-related use case characteristics* and then rate subsequent dimensions accordingly. Again, Excel converts these numbers into percentages in the background so that all of the amenability dimensions total 100%. Upon completion of this step, a final amenability score results. A final score of 0 corresponds to a factor of 1. Thus, a final score above 0 corresponds to a factor above 1, indicating an amplification of a use case's amenability. Conversely, a final score below 0 corresponds to a factor below 1, suggesting a reduction in a use case's amenability to decentralized ID.

Upon completing Tiers I and II, you may proceed to the *Summary* tab to view the overall use case amenability score, including its breakdown into the six dimensions visualized in an amenability summary chart. That section's information will provide a basis for follow-up discussions with your senior executives and other MVE stakeholders you might approach in the subsequent steps. To get a comprehensive overview of Tier II, including technology and market statements, visit the *Detailed view of Tier II* tab located next to the *Summary* tab. Red highlighted cells signify either the top 10% statements of critical importance or the statements that you gave a rating of -1 or lower, requiring extra attention during implementation.

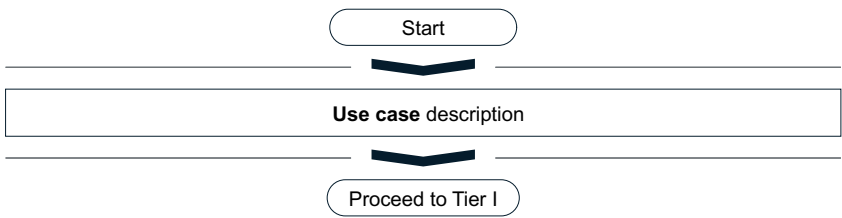


Final amenability score		0.00
Use case dimensions		Amenability factor
Human-related use case characteristics		0.00
Organization-related use case characteristics		0.00
Technology-related use case characteristics		0.00
System-related use case characteristics		0.00
Collaboration-related use case characteristics		0.00
Wider macro-economic-related use case characteristics		0.00

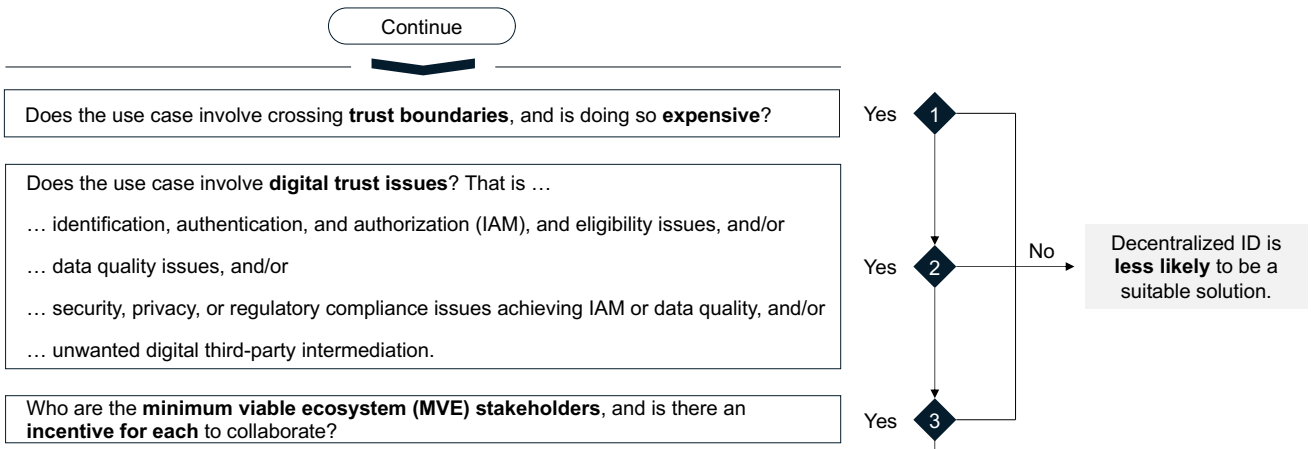


3 Assessment Framework Overview

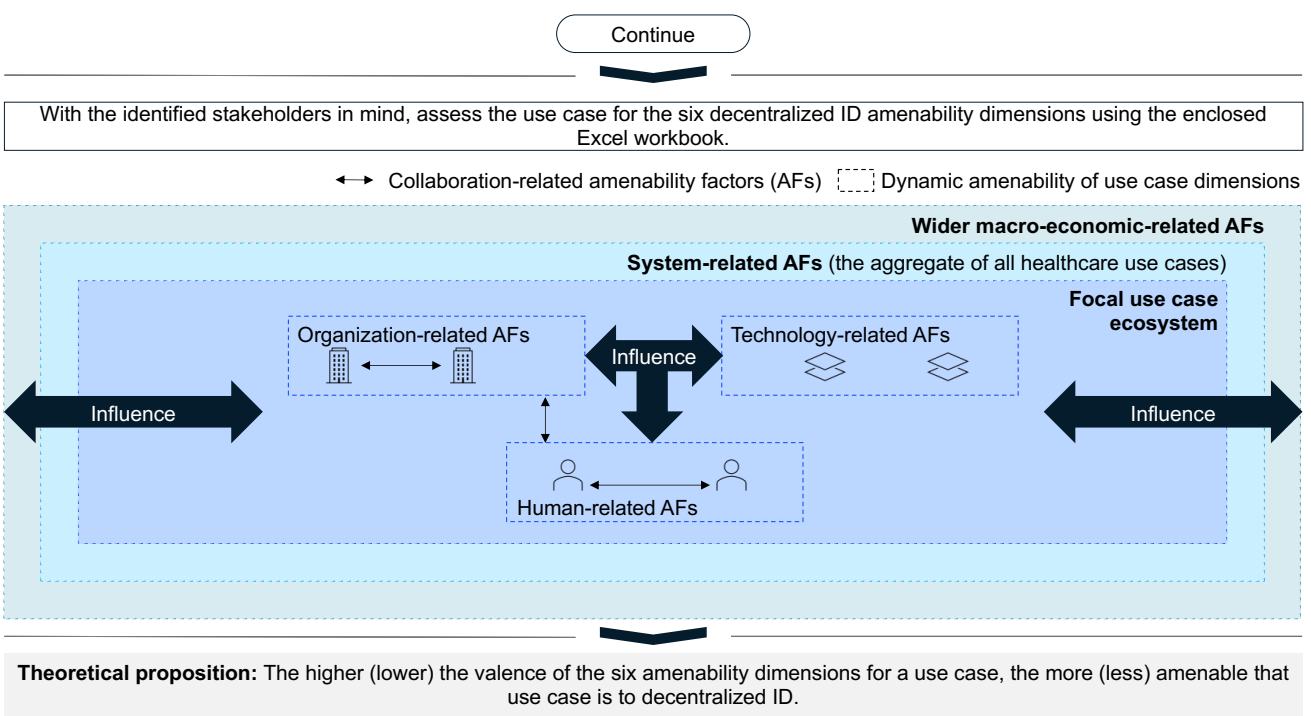
Preparatory step



Tier I: Critical amenability assessment



Tier II: Comprehensive amenability assessment



4 The Decentralized ID Checklist Toolkit Overview

The Decentralized ID Checklist toolkit comprises various components that will aid in your use case assessment and the potential launch of a decentralized ID implementation endeavor.

- ▶ **An analytical tool:** The core tool in Excel format, designed to facilitate the population and final score calculation of the framework. The workbook has two parts – input and output – with the latter summarizing and analyzing all the inputs and thus serving as a basis for further discussion with senior executives or analogous positions and other internal and external stakeholders.
- ▶ **A companion guide:** A multi-media guide, intended to assist in navigating the framework. It comprises a textual reference manual (i.e., this very document) and a screencast, which is a 10-minute how-to video that explains the framework for a more hands-on approach to populating it.
- ▶ **A live resource wiki:** A dynamic, i.e., live document, hosted on GitHub. It offers supplementary resources to assist in addressing Tier II questions and provide a jumpstart for potential implementation.

5 Glossary

Actor	Decentralized ID is not limited to individuals but extends to actors, including for-profit and not-for-profit organizations, federal agencies, objects, and anything else requiring identification in the physical or digital world.
Amenability	The likelihood of the successful deployment (i.e., system-wide adoption and value-adding use within a set timeframe) of decentralized ID in the US healthcare system.
Deployment	The umbrella term for technology adoption and use. The term <i>use</i> is to be understood as synonymous with “implementation.” Thus, deployment encompasses the entire innovation adoption process from the adoption decision to implementation, which involves integrating the technology into an actor’s operations to the extent that it is no longer novel. It is assumed that the scaling of the technology is a result of system-wide adoption and value-added use, with both acting as preconditions.
Decentralized ID	Decentralized ID refers to the concepts, ideas, architectures, processes, and technologies that facilitate inclusive, inherently, and mutually trustworthy digital relationships that instigate power-structure changes and are collective-action- and network-dependent to reach their full potential.
Ecosystem	An ecosystem is defined by the alignment structures of the multilateral set of actors that need to interact in order for the use case to materialize and be addressed. Multilateral refers to the relationships between two actors that are themselves dependent on all other relationships within the ecosystem such that these relationships cannot be broken down into bilateral interactions. Although a set of actors implies the involvement of more than one actor, it does not necessarily mean that the set is complete and unchanging.
End-user	The US healthcare system stakeholder that will interact with the decentralized ID solution(s).

Evidence	Past experiences, knowledge, policies, certifications and accreditations, computer configurations, and contracts such as the HIPAA BAA. Evidence is characterized along three dimensions. Within a given context, it needs to be sufficient, appropriate, and persuasive.
Minimum viable ecosystem (MVE)	Represents the minimum stakeholders and stakeholder groups necessary for the use case to materialize and be addressed. It serves as the catalyst for the joint endeavor, forming the foundation for further ecosystem development.
Relevance	The costs associated with the current way of (1) verifying and proving ID, authenticity, authorization, and eligibility and (2) achieving use-case-appropriate data quality (3) in a secure, privacy-preserving, and regulatory-compliant manner. The nature of these costs can differ depending on the actor and use case and may encompass financial expenditures, time expended, and effect on user satisfaction, which ultimately affect the bottom line.
System-wide adoption	The achievement of perceived critical mass, which signifies the point at which existing and potential decentralized ID adoption decision-makers and users have the perception of whether the decentralized ID solution has a critical mass of users through interactions with others.
Trust	There are various definitions of trust, but for the purpose of this framework, the following definition is employed: “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al., 1995, p. 712). While not explicitly accounted for in this definition, it is worth noting that trust involves vulnerability and inherent risk.
Trustworthiness	Can be understood as deserving of trust (Cambridge Dictionary).
Trust boundary	Characterizes the evidence that regulates interactions between you and other actors within the trust boundary. Within the trust boundary, the evidence is sufficient, appropriate, and persuasive enough for you to engage in trustworthy interactions with the evidence-providing actor (i.e., the other party). Actors on this side of the boundary are considered trustworthy. Beyond the trust boundary, the provided evidence is insufficient, inappropriate, and unpersuasive for you to engage in interactions with the evidence-providing actor. Actors on this side of the trust boundary are deemed untrustworthy. For a trustworthy digital interaction to happen, these actors need to be brought within the trust boundary through verifiable evidence. Even if the audit standards (i.e., the sufficiency, appropriateness, and persuasiveness of the evidence required and provided) are exceedingly high, trust is never anticipated to be zero unless the interaction is solely among non-human actors (i.e., things). This is because trust is still needed in the actors within the trust boundary to comply with the evidence provided. Establishing these trust boundaries can be economically costly. The trust boundary for a particular interaction, and thus your willingness to bear risk, is determined by four factors: (a) the context of the relationship, (b) the probability of the process failing, (c) your expected return, and (d) the cost you are willing to incur to mitigate risk and enhance confidence in the outcome. Given the dependence of trust on these multiple factors, these trust boundaries are in flux.
Use case	In general, use cases, as a form of writing, describe a set of actions that actors need to perform jointly to achieve a certain goal. As these documents are

typically read by non-technical individuals, they are often written in a textual format (Cockburn, 2001). Use cases are always named using verb phrases in the present tense. Prime examples of decentralized ID use cases across healthcare include Facilitate Medication Prescriptions, Prescribe Medication for Patients, Prove and Verify IDs and Insurance Coverage, Recruit Participants for Clinical Trials, and Prove and Verify Physician Credentials.

Value-adding use	The extent to which a technology is utilized within a specific context to maximize and harness its full potential.
------------------	--

6 References

- Cambridge Dictionary. Trustworthy. Retrieved November 26 from <https://dictionary.cambridge.org/dictionary/english/trustworthy>
- Cockburn, A. (2001). *Writing effective use cases*. Addison-Wesley.
- Cummings, J. L., & Holmberg, S. R. (2012). Best-fit alliance partners: The use of critical success factors in a comprehensive partner selection process *Long Range Planning*, 45(2-3), 136-159. <https://doi.org/10.1016/j.lrp.2012.01.001>
- Flessa, S., & Huebner, C. (2021). Innovations in Health Care—A Conceptual Framework *International Journal of Environmental Research and Public Health*, 18(19), 10026. <https://doi.org/10.3390/ijerph181910026>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709-734.