|  |  |
| --- | --- |
| **Human-related AFs** | |
| Prior information technology experience | End-users and/or decentralized ID adoption decision-makers have a positive or neutral experience with IS (including blockchain). |
| Expected workload | The workload of the decentralized ID solution’s end-users is not expected to increase. |
| Change in workflow | The workflow of the decentralized ID solution’s end-users is not expected to change. |
| Perceived legislative compliance | Decentralized ID is perceived as compliant with federal and state-specific legislation, such as HIPAA or the 21st Century Cures Act. |
| Patient and immediate lay caregiver engagement | The patients and/or immediate caregivers (e.g., family members) do not have to engage more and/or incur additional costs compared to the status quo. |
| Subjective trust in digital medium | The notion that the perception of a technology’s security relies on circumstantial information (e.g., opinions of friends and family, company reputation, etc.) rather than the technology’s inherent security features and actual capabilities can be addressed. |
| Data subject privacy and security concerns | Data subjects involved perceive data movement and ubiquity as a desirable state. |
| Generational divide | The generational divide of the end-user population can be addressed. |
| User input design | The end-users can play an active role in the design of the decentralized ID solution. |
| Job insecurity | No job positions within our organization are expected to be discontinued upon decentralized ID introduction. |
| **Organization-related AFs** | |
| Expectation management | There is a clear organizational understanding of what decentralized ID can and cannot do. |
| Endeavor-strategy alignment | The purpose of the endeavor aligns with our organizational strategy and the long-term benefits are expected to outweigh the costs in the ratio mandated by our organization. |
| Digital agency | Our organization can make decisions regarding the adoption of general IS without being subject to the will of external stakeholders. |
| Investment appraisal | An investment appraisal framework can be developed to help evaluate broad concepts such as decentralized ID that can be implemented in several ways against the status quo and alternative investment options. |
| Innovation pace | Our organization is willing to embrace a phased approach to decentralized ID adoption as opposed to expecting an immediate paradigm shift. |
| Resource availability | Resources (e.g., budget, facilities, employees, and/or talent pool knowledgeable about decentralized ID, training, technical support, etc.) are accessible and will be made available when needed. |
| Internal sponsorship | The endeavor has clear, readily identifiable sponsorship reflective of its importance within our organization, and some of these internal sponsors may act as boundary spanners who can influence other organizations necessary for the MVE to collaborate. |
| Organizational/cultural change | The endeavor does not require any substantial organizational and/or cultural change and is not expected to be impacted by major organizational/cultural change, such as a leadership transition. |
| Operational change | Existing operational processes can be extended as opposed to overhauling them. |
| Collaboration willingness | Our organization is willing to collaborate with other organizations (including competitors) on a solution for the identified digital trust problems that cannot be solved independently. |
| Externally generated data trust | Our organization is willing to trust, rely on, and make use of externally generated data. |
| External data access | Our organization is willing to allow other MVE members to access our data through patients and make this data legible elsewhere. |
| Piloting | Our organization is willing to engage in decentralized ID pilots aimed at testing solutions that will handle highly sensitive and confidential data. |
| **Technology-related AFs** | |
| Technology qualities | The decentralized ID solution can be developed to be available, dependable, secure, adaptable, and flexible as local needs and context change. |
| Information quality | The information provided through the decentralized ID solution can be made legible and relevant. |
| Existing standards | Use case-appropriate decentralized ID standards exist. |
| Existing minimum viable solution | A decentralized ID minimum viable solution already exists that can be leveraged. |
| Decentralized key management | Robust decentralized key recovery solutions exist that can be leveraged and adhere to the following criteria: they (a) do not have any centralized authority to fall back on for a “password reset” option, (b) do not come from a single entity or consortium, (c) do not dictate a single cryptographic algorithm or cipher suite that everyone must use, (d) the keys and wallet data are portable across multiple decentralized identity providers, and (e) do not assume any specialized knowledge or skills from the end-users. |
| Offline access | The decentralized ID solution can be provided offline, even with sporadic or uncertain connectivity. |
| Interoperability | The infrastructure for interoperability, in terms of scalability across different use cases and interchangeability of decentralized ID solution providers, is mature. |
| Integration | The organizational stack does not require significant change and the decentralized ID solution can be seamlessly integrated into our organization’s current systems. |
| Transition period | The decentralized ID solution can run in parallel with the legacy system until it is institutionalized. |
| Technical literacy | No special technical literacy is required from the end-users. |
| Phishing opportunities | Accidental data disclosure from end-users and phishing attempts from malicious counterparties can be prevented. |
| Back-end implementation | The decentralized ID solution will be a matter of a back-end implementation to an existing tunable front-end. |
| User-friendly interface | An end-user-friendly interface for the decentralized ID solution can be developed. |
| Sustainability | The decentralized ID solution can be deployed sustainably. |
| **System-related AFs** | |
| Digital trust problem spread | The digital trust problem(s) identified in Tier I are shared with across and within several stakeholder groups of the healthcare system, to provide the leverage for network effects to propel the decentralized ID solution to ubiquity. |
| Pull-innovation | End-users are demanding a solution to the use case’s digital trust problem(s). |
| Peer pressure | Our business partner(s) require us to adopt decentralized ID infrastructure to be able to do business with them. |
| **Wider macro-economic-related AFs** | |
| Media | The media and wider public have no negative opinion about decentralized technologies. |
| Regulatory frameworks | Federal and state efforts and laws relevant to the use case do not work in opposition to one another. |
| **Collaboration-related AFs** | |
| Scope and vision | The scope and vision of the endeavor can be well defined. |
| Equivalence | The MVE stakeholders can collaborate on an equal footing, wherein they bear a comparable level of risk, distribute the expected workload equally, and enjoy equivalent benefits. |
| Comparability | The MVE stakeholders have comparable innovation capabilities, such as budget. |
| Resource complementarity | The MVE stakeholders have complementary resources, and there is minimal resource redundancy. |
| Strategic fit | The MVE stakeholders have a compatible strategic views and orientation. |
| Cognitive alignment | The MVE stakeholders share comparable perceptions and perspectives regarding the endeavor and its context. |
| Organizational fit | The MVE stakeholders have compatible organizational structures. |
| Operational fit | The MVE stakeholders have compatible operations. |
| Cultural fit | The MVE stakeholders have compatible organizational culture. |
| Human fit | The backgrounds and experiences of the in the MVE involved employees are compatible. |
| Tech stack fit | The MVE stakeholders have compatible tech stacks. |
| Disintermediation | The MVE does not involve stakeholders who may act as change resistors due to potential losses from disintermediation or significant negative effects on their current business model. |
| Cold-start problem | The MVE includes stakeholders who are willing to be system pioneers. |
| Shift in power structures | The endeavor does not involve a major change in the power structure among MVE stakeholders. |
| Perverse incentives | Perverse incentives of MVE stakeholders are acknowledged and can be addressed. |
| Regulatory body | The federal agency(ies) with regulatory responsibility for the use case can be clearly identified. |
| Regulatory interest alignment | The endeavor aligns well with the goals (e.g., interoperability) of the identified federal agencies. |
| Regulatory support | Regulatory support is necessary in the form of mandates, enforcement, or financial incentives, and the federal agencies are willing to provide such support. |
| Medicare support | Support from Medicare, the governmental-run and -sponsored agency that is widely recognized as the driving force behind healthcare reform, is not required. |

a *End-user* refers to individuals part of the US healthcare industry that will interact with the decentralized ID solution(s).

b An 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 the further development of the ecosystem.