walt.id

The Pilot Playbook.

Building Pilots with Self-Sovereign Identity.

Table of Contents

About the Playbook

This playbook will help you plan and scope your pilot projects using Self-Sovereign Identity (SSI). For this purpose, the playbook is divided into 5 chapters:

1. **Identify use cases**: A framework and examples will help you discover opportunities to create value for your organisation and stakeholders.
2. **Select use cases**: A matrix and different selection criteria will help you analyze and prioritize opportunities based on your strategy and requirements.
3. **Select ecosystems**: An elaboration of identity ecosystems and a simple approach for selecting the right one(s) based on your organisation's operating model.
4. **Plan your Implementation:** Guidance for setting project requirements, technology selection and answering the question of "buy or build".
5. **Implement your Pilot:** Tips to make sure you get the most out of your pilot project.

Before you start ...

Are you already familiar with Self-Sovereign Identity (SSI) and its concepts?

If you are not (sure), we recommend reading about the basics of SSI before diving into the playbook, because once you have a rough mental model of how SSI works, it will be easier for you to apply learnings from this playbook.

To help you, we published various articles like an "Introduction to Self-Sovereign Identity" or an "Introduction to Ecosystems". You can find everything you need on our website.

Chapter 1 | Identify Use Cases

This chapter is about gaining clarity about and defining your goals from a business perspective, which is crucial if you want to successfully identify opportunities where Self-Sovereign Identity (SSI) can significantly improve various areas of your business.

The following sections will guide you through the process and provide you with helpful tools like an *Opportunity Framework* and *Inspirational Use Cases*.

Multi-Party Processes

As a first step, analyze your existing business processes with a focus on multi-party interactions, such as interactions between your organisation and your citizens, customers, employees, consortium partners, suppliers or any other stakeholders.

While SSI can create significant value in interactions between only two parties (like your organisation and your customers), the more stakeholders involved the better considering that multi-party processes are inherently challenging to support with existing centralized systems.

Opportunity Framework

To identify and further narrow down opportunities for leveraging SSI, it is helpful to focus on specific categories or areas of your operations. The following framework offers generic examples and guiding questions to help you on your journey.

Category	**Guiding Questions**	**Yes / No***
User Experience	Do your customer onboarding processes require the use of passwords, online forms, multi-step identity verification processes or other sources of friction? *SSI can streamline user journeys and flows by replacing existing multi-step processes with a simple 1-click process.*	
Data Quality	Do you face data quality or data consistency issues, for example, because customers often provide wrong information (intentionally or due to typos in forms)? *SSI can ensure high data quality based on identity information verified by trusted third parties.*	
Security	Do you use passwords, store sensitive / personal data in a centralized fashion or wrestle with the elimination of other attack vectors?	

	SSI can enable more secure authentication and identification while ensuring data minimization and decentralized storage.	
Privacy & Compliance	Is regulatory compliance (GDPR, CCPA) an ongoing challenge or do procure third-party solutions to ensure compliance? *SSI can facilitate compliance via user-centric data and consent management or automatable fulfillment of data provision requests.*	
Process Automation	Do you struggle with process automation that would benefit from machine-readable stakeholder data? *SSI can unlock reliable and machine-readable stakeholder data to power enhanced process automation.*	

** A "yes" means that SSI can positively impact this business area.*

Note that this framework does not provide a definitive list or includes every possible application category of SSI for your organization. You will likely discover additional areas specific to your organisation or industry.

Inspirational Use Cases

Often it is helpful to consider use cases which are typical for your industry or which have already been implemented by others. You can find a list of use cases for different verticals below:

Industry	**Exemplary Use Cases**		
Public Sector	Seamless remote access to eGov services and data provision.	Digitisation of documents (e.g. passports, ID cards, drivers license).	Remote application for / verification of visas, work permits, professional licenses.
Education	Remote student onboarding.	Digitisation of grades lists, diplomas, student IDs.	Facilitation of (cross-border) student mobility.
Employment (Recruiting / HR)	Seamless job applications.	Instant background checks of employees and contractors.	Maintenance of employee and contractor data.

Financial Services	Customer verification (KYC/B).	Remote account opening.	Streamline loan applications / lending.
Insurance	Frictionless customer onboarding.	Seamless access to insurance products, incl. micro-insurance.	Individual insurance rates based on verifiable health data.
eCommerce	Frictionless check-out.	Vouchers, discounts (e.g. for students)	Proof of age (e.g. tobacco, alcohol).
Travel & Mobility	Application / verification of visas.	Hotel booking and check-in/out.	Vaccination proofs, transportation tickets.
Health Care	Proof of insurance.	Digital prescriptions and medical reports.	Proof of vaccination.
Supply Chain	Verification of product authenticity.	Verification of product provenance, lifecycle.	Verification of vendors, other actors.
Marketplaces	Frictionless user onboarding and authentication.	Fraud prevention via user verification and identification.	Automated data provision (right to access).

Chapter 2 | Select Use Cases

Once you have a list of all opportunities or use cases, start prioritizing them based on your organization's strategy, challenges and product or service portfolio.

Prioritization Matrix

The following matrix offers a simple way to prioritize your use cases and decide which pilots you want to implement early on based on their (1) impact on your organisation (2) ease of implementation.

High Impact	Put on Roadmap *"Impactful Transformation"*	Build a Pilot *"Low Hanging Fruit"*
Low Impact	Disregard *"Don't Touch"*	Put on Roadmap *"Nice New Feature"*
	Hard to implement	**Easy to Implement**

The following sections will provide more context with regards to the criteria applied in the matrix:

Impact

The most important criteria for the selection of your use case is its potential impact on your organisation. Consider the following generic benefits of SSI when applied to different use cases:

- **Increase revenue**: Streamline user flows such as by eliminating passwords, forms or multi-step identification during onboarding or check-out processes to increase conversion or lower dropout rates.
- **Lower costs**: Enable online interactions that conventionally required in-person meetings or automate business processes to save internal costs and personnel resources (e.g. for manual data processing) or even replace third-party services you are currently using to solve related issues with a single, unified solution.

- **Prevent compliance issues**: Facilitate regulatory compliance especially with regards to personal data processing (e.g. based on the EU General Data Protection Regulation, GDPR) to avoid high penalties and brand damage.
- **Prevent fraud**: Ensure reliable stakeholder and identity verification and introduce tamper proof digital documents to prevent identity theft or document forgery.
- **Mitigate security risks**: Eliminate main risk factors that cause data breaches such as passwords or aggregated data storage.
- **Strengthen your brand**: Offer more seamless user experiences while strengthening security and enhancing privacy by giving your stakeholders control over their data.
- **Prevent falling behind competitors**: Finally, consider the impact on your business if competitors adopt SSI before you do.

Ease of Implementation

The effort required to implement your pilot can significantly vary depending on factors like the scope or the chosen development approach. For example, you can develop “standalone pilots” to showcase simple SSI-based functionality for a specific use case with a low-to-no-code approach. Alternatively (or subsequently) you can develop pilots which are integrated with your target IT infrastructure to show more sophisticated use cases and extensive capabilities.

Independently of which approach you choose for implementing your pilot project (standalone vs. integrated), your analyses should go beyond the pilot implementation and already consider requirements for production settings to ensure that the use case(s) you pick can also be effectively implemented in production if your pilot is a success.

In order to classify the ease of implementation, the following criteria may be considered:

- **User Interface**: How much effort is required to enable users to interact with the new system? How do different actors in a use case interact? (Answers may range from command line tools or web service calls (backend) to fancy native mobile app User Interfaces).
- **Data**: What kind of data will you use? Where and how is data currently stored and processed? Does the (test) data need to be anonymized (due to regulatory requirements)?
- **Deployment**: How will the solutions be deployed and hosted? Which environments are used and what are the system requirements (for staging, testing and production)?
- **Integrations**: How complex are the business processes and which IT infrastructure and applications are currently involved in the process?
- **Ownership**: Are different departments involved in the use case or pilot implementation? If yes, what is the structure for decision making and how will this affect the implementation (beyond the pilot project)?
- **Buy or Build:** What building blocks for creating the pilot are required and how is the workload distributed among internal or external teams? Furthermore, what existing open

source components can be utilized for free. *(For more information on this topic see "Chapter 4 | Plan your Implementation".)*

Anticipated Regulatory Compliance

There is one more criteria to be considered which is not directly listed on the matrix but may strongly influence your impact analysis:

In June 2021, the European Union proposed an amendment to the European eID framework ("eIDAS") that will create a European digital identity ecosystem with far reaching implications. For example:

- European governments will be obliged to provide citizens with digital identity solutions via so-called "wallets".
- The private sector will be required to use strong user authentication based on such "wallets" across industries, including transport, energy, banking and financial services, education, social security and health care, telecommunications, and very large online platforms among others.
- The regulation will have to be implemented within 1 year after the proposal's approval.

It is expected that the use of Self-Sovereign Identity (SSI) will ensure compliance with this new eIDAS regulation if procured SSI solutions integrate with the EU Blockchain Service Infrastructure (EBSI) and comply with the standards of the European Self-Sovereign Identity Framework (ESSIF).

You can find the regulatory proposal here.

Chapter 3 | Select an Ecosystem

Once you have determined the use case(s) you want to implement, it's time to select an identity ecosystem, preferably the one you want to join after you completed your pilot project.

Choosing an identity ecosystem is vitally important because it will have a major impact on whether you can actually achieve your business goals as well as on the technical planning and implementation of your project, including technology selection.

What are identity ecosystems and why are they important?

Even though Self-Sovereign Identity (SSI) is based on global standards, different ecosystems exist and each ecosystem uses SSI in a different "flavour". A main reason for the existence of different SSI flavours is the fact that different supranational organisations (like the European Union), governments or private sector alliances usually have different views and requirements on how their respective ecosystems should work.

So-called "Governance and Trust Frameworks" illustrate this more clearly: These frameworks determine the rules by which an ecosystem is governed to ensure that different parties that operate in an ecosystem can trust in and reliably verify each other's digital identities.

The European Union, for example, established its own identity ecosystem based on the European Self-Sovereign Identity Framework (ESSIF) which is aligned with European regulations like eIDAS or the GDPR (General Data Protection Regulation) and considers the specific needs of a coalition of 27 governments. Governments in the Americas, Asia, Africa or private sector consortia will make different decisions when defining the governance structure of their national or industry-specific ecosystems as they have different goals and requirements.

How to choose an identity ecosystem?

On a high-level, we can distinguish two types of ecosystems:

Regulated Ecosystems

This type is based on laws created by supranational organisations and/or individual governments. The governance structure of these ecosystems is tightly integrated with regulations in various fields such as data protection, privacy, security and digital infrastructure.

Though the only viable example today is the emerging European digital identity ecosystem based on the European Self-Sovereign Identity Framework (ESSIF), other regulated ecosystems will likely emerge over the next few years based on Europe's example.

Unregulated Ecosystems

Unregulated ecosystems are based on contractual rules and obligations, not regulations. They are only binding for organisations and individuals who consent to the Governance and Trust Frameworks. These ecosystems are usually created by private entities like industry consortia

which is why their governance structures are often determined by industry or even use case specific requirements.

An example is the “Velocity Network”, which is a global ecosystem for recruiting and human resources (HR) that aims to establish the “internet of careers”.

Conclusion

The biggest difference between regulated and unregulated ecosystems is that the former (regulated) always prevails over the latter (unregulated) if there is a case of conflict. Therefore unregulated ecosystems mainly serve the purpose of complementing regulated ones, such as to enable SSI where no regulatory standards and rules exist.

At the end of the day, your ecosystem selection will depend on the markets you are operating in:

- If you operate in a market for which a regulated ecosystem exists, you will have to comply with this ecosystem’s standards and governance framework. However, you may also adopt unregulated ecosystems that complement or extend it.
- If no regulated ecosystem exists for the market you address, you may join unregulated ecosystems, while monitoring regulatory activity to scout emerging regulatory standards early on and ensure long-term compliance.

Special note for organisations operating in Europe:

Every European business or public authority should evaluate and ensure compliance with the new European digital identity ecosystem, i.e. with the EU Blockchain Service Infrastructure (EBSI) and the EU SSI Framework (ESSIF).

It is expected that compliance with EBSI and ESSIF will ensure compliance with a new regulatory proposal by the EU that will force the adoption of user-centric identity across Europe (based on an amendment of the eIDAS regulation). Also, ESSIF’s emerging technical standards ensure interoperability across European borders and across industries as well as provide a robust governance framework to ensure highest levels of trust and accountability.

Chapter 4 | Plan your Implementation

Once you have selected your use case(s) and ecosystem(s), start planning the actual implementation of your pilot project. The following sections offer a blueprint to guide you through the planning phase.

Determine Requirements

At the end of the day, your project requirements will be strongly influences by your selection of

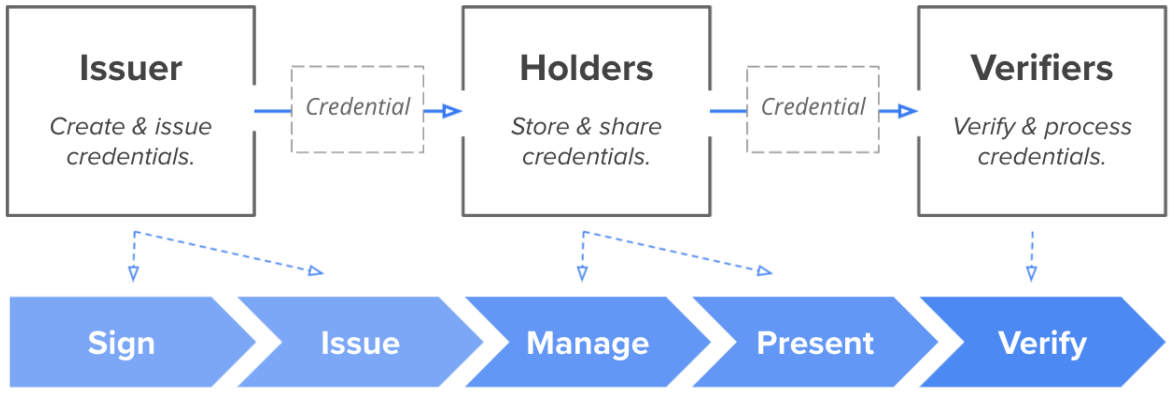
- use case(s) - which provide the high-level goal of your project and determine the role you will assume in an ecosystem,
- ecosystem(s) - which will require a certain type of implementation or “flavour” of Self-Sovereign Identity (SSI).

Role-Specific Requirements

SSI enables identity ecosystems in which individuals and organisations can share data seamlessly, securely and privately. To render this possible, SSI ecosystems look like three-sided marketplaces, in which participants can take on three different roles:

- **Issuers**: Parties who already store identity-related data of others (e.g. of citizens, customers, employees). They are the data sources; usually organisations.
- **Holders**: Parties who receive data about themselves from Issuers. They can store, manage and share data freely; usually individuals and organisations .
- **Verifiers**: Parties who rely on data to provide products and services. They verify and process data that has been provided by Holders; usually organisations or individuals in their professional capacity.

The three roles required for SSI ecosystems:



Note that a single party can act as Issuer, Holder and Verifier depending on the use case. For example, a university may issue diplomas to graduates (Issuer), manage their own accreditations (Holder) and request education records from incoming students (Verifier).

The following table will help you determine the role your organisation will assume.

Role	Guiding questions	Yes / No
Issuer	Do you plan to “issue” data (identity credentials) to your citizens, customers, employees or other stakeholders?	
Holder	Do you plan to manage and/or share your (organisation’s) data with someone else? *Note that you will almost always assume the role of a “Holder” considering that most interactions will require mutual authentication or identification.*	
Verifier	Do you plan to request and verify data from others to authenticate or identify them (e.g. for the purpose of providing products or services)?	

Ecosystem-Specific Requirements

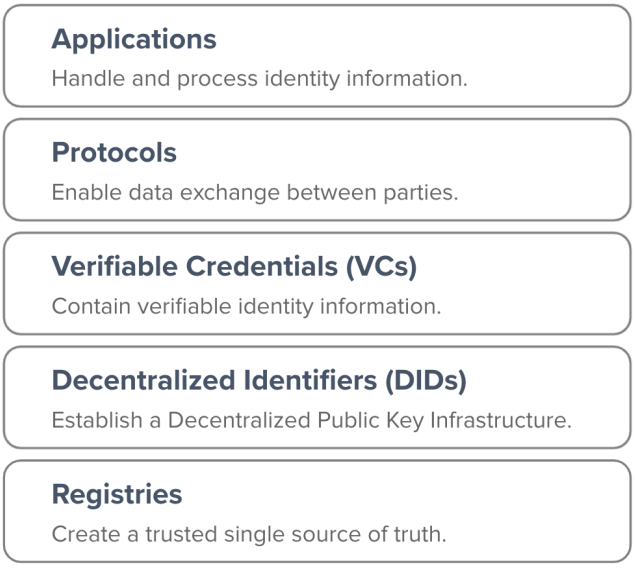
Different ecosystems require different functionality depending on the technical standards and governance systems they are based on. Typically the impact of your ecosystem selection will span over different layers of your implementation. For example:

1. **Registries**: Which blockchains or other technologies are used to create registries and how do they work?

   How does the ecosystem create a single source of truth to establish trust between different parties?

2. **SSI Flavour**: Which SSI flavour is used by the ecosystem?

   What are the technical specifications and standards for core building blocks like Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and data exchange protocols and how are they used by applications?



As a result, when building a pilot or evaluating technologies, ensure that your setup supports the requirements put up by the ecosystem of your choice with regards to registries and SSI flavours.

The following example illustrates high-level implications of ecosystem selection for the case of the European ecosystem (EBSI, ESSIF):

Example: European Ecosystem (EBSI, ESSIF)		
	Ecosystem-specific requirements	Implications
Registry	European Blockchain Service Infrastructure (EBSI), a permissioned Ethereum Blockchain (Quorum/Besu).	Projects must be able to interact with / support EBSI.
	Non-exhaustive lists of EBSI Registries: ● Trusted Issuer Registry (TIR): Contains information about verified "Issuers" (mainly organisations) to enable data verification. *Examples: Universities or banks.* ● Trusted Accreditation Registry (TAOR): Contains information about organisations who accredit "Issuers" in regulated industries. *Example: Ministries that accredit universities to issue certain types of diplomas.* ● Trusted Schema Registry (TSR): Contains data models and templates for credentials to ensure e.g. semantic interoperability.	Solutions are required to support concrete specifications and standards of the implemented registries, incl. data models, flows and business logic, in order to enable registry interactions.
SSI Flavour	DID method called "did:ebsi" with a specific data model and business logic for anchoring and resolution of DIDs on EBSI.	Projects must support "did:ebsi", incl. flows for anchoring and resolution.
	VC types include so-called "Verifiable IDs" and "Verifiable Attestations" with specific semantics and data models as well as requirements for signatures, issuance and verification.	Projects must support different types of VCs with specific data models and flows for issuance, verification.
	Protocol for data exchange based on OpenID Connect (OIDC) / Self-Issued OIDC Provider (SIOP).	Projects must support specific data exchange protocols.

Contact us if you want to learn more about the specific requirements of the emerging European identity ecosystem (EBSI, ESSIF).

Data-Specific Requirements

There will be certain requirements with regards to the data that ought to be utilised in the course of your pilot project and they may differ strongly depending on your use case(s) or ecosystem(s).

Therefore, it is important to clearly identify which data will be used in the course of your project and how this data will be used, especially how data will be transformed into VCs.

Two decisions are particularly important in this context:

- **Formats**: The data format will likely be determined by the ecosystem of your choice. Depending on ecosystem specifications, different formats may be allowed, such as JSON and/or JSON-LD. The selection of the format will have far reaching technical implications such as with regards to machine-readability, signature or proof types.
- **Ontologies and templates**: Data ontologies and templates of specific VCs may also be determined by your ecosystem - or at least certain rules and minimum standards. If this is not the case, make sure to define them as required by your use case and stakeholders.

Technology Selection

Once the high-level requirements for your pilot project are set (role-, ecosystem-, data-specific), it is time to take a closer look at the technology.

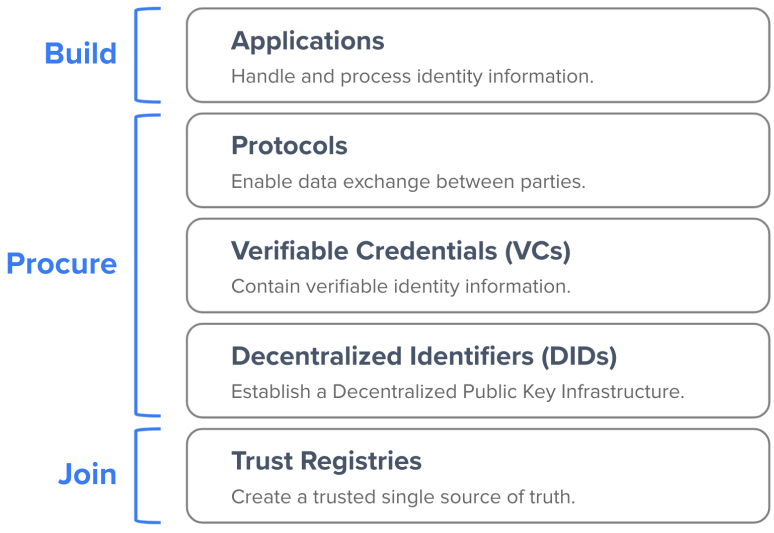
Buy or Build?

When planning your implementation, you face a tough question of whether you should (1) build your own, custom solution or (2) procure and use existing ones?

Finding an answer will be a complex challenge, but there is one thing you should keep in mind: Building Self-Sovereign Identity (SSI) solutions from scratch is an uneconomical and (in most cases) even infeasible undertaking because it requires extensive knowledge about a number of novel and fast-changing technologies (e.g. DLTs, DPKIs,, cryptography, authentication protocols, etc.) and new standards (e.g. DIDs, VCs). The likely result will be months to years of development with a high risk of failure.

Therefore, we suggest screening the market for existing infrastructure solutions and frameworks that fit your requirements and then either to procure them or opt for a “hybrid” approach, in which you build on top of these solutions. In short:

1. **Join ecosystems** (Registries, Governance Frameworks).
2. **Procure SSI infrastructure** (that supports the right SSI flavors).
3. **Build applications** (inhouse or with vendors and partners).



Technology Selection Framework

Technology selection can be complex and will have a large impact on your organisation. To facilitate this process and ensure that you end up with the right solutions, we distilled five criteria against which we recommend to scan every implementation you consider to use:

1. **Ecosystem & Interoperability**

Probably the most important factor in your decision making process is a solution's ability to support the ecosystem(s) that you will join based on your business strategy.

If a solution does not support the technology framework, specifications and business logic required by your ecosystem selection, there is not much this solution can offer you.

2. **Open Source vs. Closed Source**

Another important questions is if a solution's source code is open source or not given the benefits of open source solutions over closed alternatives such as:

- Prevention of dependencies and vendor lock-in
- Prevention of legal risks and administrative burdens
- Transparency with regards to quality and security
- Faster and straightforward adoption
- Lower costs

If you decide to use open source solutions, make sure to carefully evaluate the licenses, because not every open source license comes with the benefits described above. As a rule of thumb, always prefer permissive licenses like MIT or Apache 2 over less permissive ones like GPL or other licenses that may contain clauses that are incompatible with your project or goals.

3. **Deployment Options**

Make sure to pick a solution that is flexible enough to support your operational strategy. Think about where and how you want to run your (identity) infrastructure for the next 3 to 10 years.

If you prefer and have the capacity (know-how, personnel) to deploy and maintain solutions in-house, either on your own servers (on-prem) or in your own cloud environment, the solution you select should support this modus operandi. The same is true if you prefer to outsource operations and consume SSI as a managed cloud service.

4. **Integrability**

Make sure to evaluate the fit between your existing IT infrastructure and the solutions you plan to procure. The better the fit, the faster, cheaper and simpler the integration and roll-out.

Make sure to conduct holistic evaluations that include every factor relevant for your integration plans: from programming languages over interfaces to "architectural openness" (i.e. a system's ability to integrate third party solutions). Make sure to prevent rip-and-replace where possible as well as vendor- or technology-related lock-in effects.

5. **Services**

Evaluate solutions not only against their technical specifications and capabilities, but also against the services which are provided to facilitate your project's success.

Relevant services include:

- Consulting (e.g. identification of use cases, project scoping and planning)
- Set-up and integration (of pilots or production systems)
- Technical support and maintenance (for your preferred deployment options).

The following framework will help you apply the five criteria:

Criteria	**Description**	**Yes / No**
Ecosystem & Interoperability	Does the solution support the ecosystems (incl. technology framework, specifications, business logic) you selected based on your business and regulatory requirements?	
Open vs. Closed Source	Is the solution open source? If yes, does it use a permissive license like MIT or Apache 2.	
Deployment Options	Does the solution support your operational strategy and preferred deployment options (e.g. self-managed on-prem or in cloud vs. managed cloud service).	
Integrability	Is the solution compatible and easily integratable with your existing IT infrastructure? Does it prevent rip-and-replace?	
Services	Is there an offering of services that will help you navigate the introduction of a new identity infrastructure and mitigate risks for your project's success? If yes, which services are offered?	

Chapter 5 | Build your Pilot & Beyond

The actual implementation of your pilot will depend on your software development approach and existing processes. Also, team selection, project management and monitoring will depend on whether you are implementing the project in-house, outsource it or opt for a hybrid approach.

Therefore, this Playbook will not offer guidance for the implementation phase such as generic project management tools. Instead we want to remind you to not lost sight of the most important things you can take with you from building a pilot:

Build-up Knowledge

Self-Sovereign Identity (SSI) is a nascent approach to digital identity that is based on novel technologies and new standards. The number of experts, particularly the number of developers who can build SSI-based solutions, is very limited. That is why it is crucial to maximise learning while building your pilot project and to hold the know-how in your organisation.

As a result, one of the most important things about setting up your pilot project is to make sure that the right people are involved. We recommend to bring in a diverse team comprised of individuals with the ability to

- understand the impact of SSI on your organisation, its units and strategy,
- understand the technologies behind SSI (enough to build solutions for your use cases),
- communicate the opportunities and implications of SSI across your organisation (including product, R&D, operations, marketing, sales, human resources and compliance teams).

Prove Return of Investment (ROI)

Apart from building up knowledge, make sure to scope and implement your pilot in a way that allows you to prove SSI's return on investment (ROI) for your organisation or unit. Keeping this in mind will help you to source the right information throughout the implementation phase and to evaluate your project in a way that will allow you to communicate its value effectively to decision makers.

As a starting point, use the results of your use case analysis from the "Prioritization Matrix" - including impact, ease of implementation and anticipated regulatory compliance. *(For more information on this topic see "Chapter 2 | Select your Use Case").*

To further strengthen your ROI analyses, put your pilot into the hands of your target groups to get early market feedback and to test your hypothesis in real-life settings.

Walt.id develops Self-Sovereign Identity (SSI) solutions for governments and businesses across industries.

Developers and organisations rely on our open source products as an easy and fast way to use Self-Sovereign Identity - including Europe's new digital identity ecosystem based on the EU Blockchain and the EU SSI Framework.

To ensure client's success, our industry-leading experts provide holistic services including from conception over the implementation of pilots and production system to enterprise support and managed cloud services.

For more information visit **www.walt.id** or get in touch via **mail**.