4

SSI Scorecard: Major features and benefits of SSI

by Drummond Reed and Alex Preukschat

By now it should be clear that SSI is not just a point technology, like Web shopping carts or mapping apps. It is a fundamental technology shift—akin to the Internet or the Web itself. As such it doesn't have just one primary feature or benefit—or even just a small set of them. Rather it offers an entire spectrum of features and benefits that vary in their impact depending on the use cases of a particular industry or application. SSI solves a digital trust problem. While digital trust is an abstract word to understand what we mean is that SSI allows for trusted interactions in the digital space where until now we had to use bandage solutions. Trusted interactions are needed on every level of the digital economy and that is why SSI can apply to almost any digital interaction where trust is needed. If you are a technical minded reader you can skip ahead to Part Two and Three which contains the deep level technical understanding for SSI, but if you want to understand the general benefits and features of SSI this scorecard will help you to define one for your own business or ideas.

The SSI Scorecardclassifies 25 major features and benefits of SSI into five categories as shown in table 4.1. In Part 4, we will use the SSI Scorecard to analyze the impact of SSI across the use cases presented for each of eight industry representative verticals.

Each category has a different combination of features and benefits that are common to SSI, but the category describes those features and benefits from a specific viewpoint or prism that we hope makes it easier to understand how wide the impact of SSI can be. The five categories are:

1. **Bottom Line:** these are features and benefits that deliver directly to a company's bottom line because of cost reduction or new revenue opportunities made possible with SSI
2. **Business Efficiencies:** the digital transformation of business is the largest impact of SSI. This category will highlight how deper re-engineering of business processes or business process automation (BPA) will be be accelerated with SSI.
3. **User Experience & Convenience:** This category will look at the same five features and benefits as the business efficiencies category, but through the lens of how they benefit the end-user.
4. **Relationship Management:** SSI will increase the trust, productivity, and value of relationships and this category explores at which levels we foresee those changes to happen.
5. **Regulatory Compliance:** Cybersecurity and cyberprivacy infrastructure will be enhanced with SSI and allow companies and people to comply with regulations.

Table 4.1: SSI Scorecard is a tool for analyzing the impact of SSI for any use case, application, industry, or vertical market.

SSI Scorecard	
Category	**Feature/Benefit**
Bottom Line	Fraud reduction
	Reduced customer onboarding costs
	Improved ecommerce sales
	Reduced customer service costs
	New credential issuer revenue
Business Efficiencies	Auto-authentication
	Auto-authorization
	Workflow automation
	Delegation & guardianship
	Payment and value exchange
User Experience & Convenience	Auto-authentication
	Auto-authorization
	Workflow automation
	Delegation & guardianship
	Payment and value exchange

Relationship Management	Mutual authentication
	Permanent connections
	Premium private channels
	Reputation management
	Loyalty & rewards programs
Regulatory Compliance	Data security
	Data privacy
	Data protection
	Data portability
	RegTech (Regulation Technology)

4.1 Feature/benefit category #1: bottom line

This category represents the easiest sale in business: features and benefits that deliver **directly to a company's bottom line**, that is, they either make a company more money or save them money—quickly. Following are five ways SSI can do that.

4.1.1 Fraud reduction

The first and fastest way SSI can help the bottom line is reducing fraud. Javelin Strategy reported that in 2016, **15.4 million consumers were victims of identity theft or fraud**, costing a total of $16 billion dollars in losses.[71] Javelin also reported that new account fraud—criminals opening up new accounts under victims' names—increased from $3 billion in 2017 to $3.4 billion in 2018.[72]

Although the potential savings from fraud reduction varies by industry segment, for some industries it is one of the largest potential sources of savings. For example, the National Health Care Anti-Fraud Association estimates that in 2017 health care fraud costs the United States about **$68 billion annually** — about 3 percent of the nation's $2.26 trillion in health care spending.

Bottom line: **even if fraud reduction was the only benefit of SSI**, it would warrant a massive investment by businesses and governments around the world. Indeed, fraud reduction is one of the primary reasons the global credit union industry is embracing SSI as its first major use of blockchain technology. See the Digital Banking chapter in Part 4.

[71] https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html
[72] https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt

4.1.2 Reduced customer onboarding costs

The cost of customer onboarding varies by industry, but in financial services in particular, the cost of Know Your Customer (KYC) compliance has gone through the roof. According to Thomson Reuters, out of 92% of the firms they surveyed, **KYC onboarding processes cost an average of $28.5 million**.[73] Ten percent of the world's top financial institutions spend at least $100 million annually on it.[74] And onboarding a new financial services customer takes anywhere from one to three months on average.[75]

There is also a steep cost for not being compliant with these regulations. In 2018, Fenergo reported that a staggering **$26 billion in fines** had been imposed on financial institutions worldwide for non-compliance with KYC, Anti-Money Laundering (AML), and sanctions regulations in the last decade.[76]

Although SSI is not a silver bullet for all the complexity of automating customer onboarding and ensuring KYC and AML compliance, it is in fact a major new weapon in this arms race—a weapon that benefits all three sides: customers, financial institutions, and regulators. By securely and privately digitizing the information required by these regulations—and enabling it to be cryptographically verified in real time with a full audit trail—SSI has the potential to save all three groups many billions of dollars annually. And it can reduce customer onboarding time from months to days or even hours.

4.1.3 Improved ecommerce sales

Statista forecasts that the total value of **global retail ecommerce will reach $3.45 trillion in 2019**—up from $1.34 trillion in 2014 and $2.84 trillion in 2018.[77] Nasdaq predicts that by 2040, **around 95% of all purchases** are expected to be via ecommerce.[78]

More than a third of online Black Friday 2018 sales were completed on smartphones.[79] But on average, only 2.86% of ecommerce website visits convert into a purchase.[80] **In fact, the global cart abandonment rate for ecommerce is close to 70%.** The Baymard Institute averaged out rates from 40 different studies, which give rates from as low as 55% to as high as 81%, to arrive at a global average of 69.89%.[81]

When you add the fact that **80% of online shoppers stop doing business with a company because of poor customer experience**,[82] the improved convenience, privacy, and safety of shopping with an SSI digital wallet means the impact of SSI on improving

---

[73] https://www.bankingtech.com/2018/09/the-future-of-client-onboarding/
[74] https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/
[75] https://www.opus.com/future-of-kyc/
[76] https://www.fenergo.com/press-releases/global-financial-institutions-fined-$26-billion-for-aml-kyc.html
[77] https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide /
[78] https://www.nasdaq.com/article/uk-online-shopping-and-e-commerce-statistics-for-2017-cm761063
[79] http://exploreadobe.com/retail-shopping-insights/http://exploreadobe.com/retail-shopping-insights/
[80] https://www.invespcro.com/blog/mobile-commerce/
[81] https://baymard.com/lists/cart-abandonment-rate
[82] https://research.hubspot.com/customer-acquisition-study

ecommerce sales is something that no online merchant can afford to ignore. As a matter of fact this can mean a revolution for the e-commerce space where digital wallets will allow for seamless authentication and payments leveling the playing field a bit with e-commerce giants like Amazon and Alibaba.

4.1.4 Reduced customer service costs

Customer service has become one of the primary battlegrounds of modern business. Gartner predicts that **89% of businesses are expected to compete mainly on customer experience**.[83]

But it is an expensive proposition. Forbes reports that **in 2018 businesses were losing $75 billion per year through poor customer service**—up $13 billion since 2016.[84] According to Infosecurity Magazine, just one persistent customer service issue—**lost passwords—costs businesses an average of over $60 per incident**.[85]

SSI can have a massive impact on improving customer experience (CX) and reducing customer-service costs. Passwordless authentication is only the start—the rest of this chapter is filled with examples such as permanent connections (no more losing track of customers), premium private channels, workflow automation, and integrated loyalty management. All of this goes straight to the bottom line—the Temkin Group reports that **even a moderate improvement in CX will boost the revenue of a typical $1 billion company an average of $775 million over three years**.[86]

4.1.5 New credential issuer revenue

All of the preceding apply to a company's existing lines of business. SSI also opens up new revenue opportunities for a surprisingly wide variety of companies. Any business whose interaction with its customers produces a measure of knowledge about their attributes and interests—or a measure of trust in their behavior—is now in a position to monetize that data in a permissioned and privacy-respecting way: by issuing their customers (suppliers, partners, contractors, and others) verifiable credentials that help them leverage this knowledge. Even better, customers themselves can be the distribution channel for this knowledge to verifiers who need it.

And verifiers will pay for that valuable knowledge for the same reason they pay for customer profile data (from data brokers), credit history (from credit rating agencies), background checks (from background verification companies), and other customer data sources today. SSI can transform this current market much the same way the Web

[83] https://blogs.gartner.com/jake-sorofman/gartner-surveys-confirm-customer-experience-new-battlefield/
[84] https://www.forbes.com/sites/shephyken/2018/05/17/businesses-lose-75-billion-due-to-poor-customer-service/
[85] https://www.infosecurity-magazine.com/opinions/how-much-passwords-cost/
[86] https://experiencematters.blog/2018/08/21/report-roi-of-customer-experience-2018/

transformed the newspaper classifieds market, the auction market, or the retail market. For example, SSI can provide the following:

- Broader, richer, and more diverse profiles of the customer than those available from third-party sources today.
- Fully permissioned and GDPR-compliant data because the customer is the vehicle for sharing the information for their own benefit.
- Fresher, richer, and more contextual data about preferences, interests, and relationships.
- Selective disclosure of attributes, data owners can choose which pieces of data they want to share, in a way that is all but impossible for direct behind-the-customer's-back data sharing agreements.

4.2 Feature/benefit category #2: business efficiencies

As important as the immediate bottom line is, SSI's larger impact will be in re-engineering business processes—a field known as **business process automation** (BPA)[87] or more broadly as **digital transformation**.[88] This kind of paradigm shift does not happen very often; it is analogous to the transition businesses underwent from snail mail to email, from phones to fax machines, and from paper to the Web.

As we illustrated in chapter 3, these efficiencies are not limited to just one area of business, but accumulate across entire workflows and even across entire industries. In this section we will look at five areas where SSI can directly impact business efficiencies.

4.2.1 Auto-authentication

Perhaps no area of Web experience is more despised by individuals and companies alike than login. The 2015 TeleSign Consumer Account Security Report said the following:[89]

- 54% of people use five or fewer passwords across their entire online life
- 47% of people use passwords that are at least 5 years old
- 7 in 10 people no longer trust passwords to protect their online accounts

In 2019 Auth0 reported that:[90]

- The average American email address has 130 accounts registered to it.[91]
- The number of accounts per user is doubling every five years.[92]
- 58% of users admit to forgetting their password frequently.[93]

---

[87] https://en.wikipedia.org/wiki/Business_process_automation
[88] https://en.wikipedia.org/wiki/Digital_transformation
[89] https://www.entrepreneur.com/article/246902
[90] https://auth0.com/learn/password-reset/
[91] http://blog.dashlane.com/wp-content/uploads/2015/07/MailboxSecurity_infographic_EN_final1.jpg
[92] http://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

- The average internet user receives roughly 37 "forgot password" emails a year.[94]

But besides the sheer hassle, the real impact of username/password-based login is the friction.

- The average person has between 7 and 25 accounts that they log into every day.[95]
- Around 82% of people have forgotten a password used on a Web site.[96]
- Password recovery is the number one request to help desks for intranets that don't have single sign-on portal capabilities.[97]

In short, by moving from conventional login to SSI auto-authentication—using an SSI digital wallet instead of a username and password—we can finally "kill the password." It will be like replacing frequent, error-prone toll booths with a wide-open, well-paved highway. Everyone can go about their business faster, more easily, and more safely.

4.2.2 Auto-authorization

Authentication (login) is just the first step in most trusted business processes. It proves that you are the rightful owner of an account. But it does not answer the next question: what are you authorized to do? What privileges should you be granted? What actions can you take?

In the world of Identity and Access Management (IAM), this is called **authorization**. It is an even harder problem than authentication. But this is where verifiable credentials truly shine. To use the analogy illustrated in figure 4.1, if verifiable credentials are a hammer, then authentication is only a thumb-tack. Authorization is a full 16-penny nail.

---

[93] http://www.marketwired.com/press-release/lunabee-survey-finds-that-17-percent-internet-users-often-forget-their-online-passwords-1850682.htm
[94] http://blog.dashlane.com/wp-content/uploads/2015/07/MailboxSecurity_infographic_EN_final1.jpg
[95] http://usablyauthentical.blogspot.com/2011/09/random-factoids-ive-encountered-in.html
[96] http://passwordresearch.com/stats/statistic97.html
[97] http://www.nngroup.com/reports/intranet/portals/

Figure 4.1: While authentication is important, authorization is actually a much bigger nail for the verifiable credentials hammer to hit.

The reason verifiable credentials are such a powerful tool for authorization is that they can solve three hard problems in one stroke:

1. **They can provide exactly the right claims needed for an authorization decision.** These decisions are made by applying the verifier's access control policies. **Attribute-based access control**[98] is based on specific attributes of the identity owner: age, gender, zip code, browser type, and so on. **Role-based access control**[99] is based on the role or roles of the identity owner: employee, contractor, customer, regulator, and so on. Either way, verifiable credentials represent the fastest and easiest way for the verifier to request and the holder to supply the precise claims needed.
2. **They can be cryptographically verified in real-time.** To be confident in an authorization decision, a verifier must trust the claims being presented. As explained in chapter 2, the whole point of SSI architecture is so a verifier's agent can verify the issuer's signature on the holder's proof in seconds.
3. **They can be bound to the holder of the credential as the authorized party.** One of the greatest sources of fraud is stolen usernames/passwords—it has grown into a $6 billion annual market precisely because they are not verifiable.[100] With verifiable credentials, there are several techniques for proving that the claims they contain were issued to the holder of the credential. These include sharing proof of a biometric for the

[98] https://www.axiomatics.com/attribute-based-access-control/
[99] https://en.wikipedia.org/wiki/Role-based_access_control
[100] https://qz.com/1329961/hackers-account-for-90-of-login-attempts-at-online-retailers/

holder and cryptographically linking credentials to a holder using zero-knowledge proofs (ZKPs) explained in our cryptography chapter.

So using a verifiable credentials model, a verifier's job can be simplified to three steps:

1. Determining the set of claims, a claim being one or or a group of data items about someone or something, needed for any particular authorization decision.
2. Determining the issuers—or the governance framework—that the verifier trusts for those claims.
3. **Making it easy for users to acquire those credentials** so the user experience is as simple and seamless as possible.

But the SSI model can go one step further in business efficiency. Once a user has established a connection with a verifier and approved sharing the claims necessary meet the verifier's policies, **the user can apply his/her own policies** to this process. For example, the user can instruct his/her agent (a device or cloud agent) to automatically share the same claims with the verifier when the user needs to repeat a business process in the future (order a supply, approve a budget, publish a web page).

Now the entire authentication and authorization process for a user—even if quite sophisticated—can be automated to the point it is carried out entirely by the user's and verifier's respective agents **including the audit trail needed for accountability**. Obviously this is a big win for users (see *User Experience & Convenience* below), but for verifiers the benefits of auto-authorization can be on the same order as the benefits of credit cards for merchants: customers can perform an essential exchange of information far more easily and painlessly, accelerating business for everyone.

4.2.3 Workflow automation

Every business process has a workflow—the series of steps that must be performed to carry it out end-to-end. Each step that crosses a trust boundary—branch to branch, customer to merchant, supplier to vendor, company to government—typically requires the authentication and authorization processes described above. So SSI agents can already wring out major inefficiencies just by performing auto-authentication and auto-authorization.

But those same agents can also **apply the business logic necessary to orchestrate the steps in the process** no matter how many trust boundaries it crosses.

This is the heart of business process automation (BPA): designing a business process so humans are doing only the steps that require their expertise, awareness, judgement, and empathy. The rest can be assigned to digital agents (who in some cases may further reassign it to robots). Besides enacting the trust infrastructure necessary to do this work safely, SSI agents are ideal for BPA because they can literally "follow a script"—in this case Javascript or a similar programming language that instructs them to apply each step in the flow of a business process. Agents can be pre-programmed with such scripts, or they can download them dynamically via SSI connections with **orchestration agents** whose job it is to maintain a library of the current scripts required for a specific business process.

SSI is a major leap forward in BPA because process improvements no longer need be limited to a single company or a single supply chain. Like the Internet and the Web, SSI enables BPA workflows to be carried out across any set of trust boundaries, according to any set of policies (governance framework) agreed to be the participants. It is truly "world wide BPA".

4.2.4 Delegation and guardianship

Digital agents can be given instructions and assigned responsibilities via program code. But most business processes require specific human workers to perform specific functions or make specific decisions as part of the process. How are those humans assigned those responsibilities?

This is the job of a subclass of verifiable credentials called **delegation credentials**. They are how a holder can prove that they have the authority to carry out a specific task or make a specific decision as part of a business process. Common examples in a corporate context:

- **Employees** can be given a delegation credential for the right to send tweets from the company's Twitter account or post new articles to the company's blog.
- **Drivers** can be given a delegation credential to pick up and deliver goods on behalf of the company.
- **Officers** can be given specific delegation credentials authorizing them to execute specific types of contracts on behalf of the company, e.g., HR officers to sign an employment contract, procurement officers to sign a purchase order, CFOs to execute a bank order, and so on.
- **Board members** can be given delegation credentials to execute electronic board votes that do not require them to be physically present for a meeting.

There are countless more examples from every context that needs to carry out business processes—governments, schools, non-profits, churches, even households. For example, parents could use delegation credentials to specify how much screen time their children are allowed, or what kinds of foods they are allowed to buy for lunch at school.

The parental example brings up another case: taking responsibility for an individual who is not in a position to wield SSI technology on their own. There are many examples besides babies or young children: the elderly, individuals with disabilities, refugees and displaced peoples, individuals without mobile phones or Internet access.

To enjoy the same rights as everyone else to self-sovereign identity, these individuals need **digital guardians**—individuals or organizations who can operate SSI agents and wallets on their behalf. This form of "complete delegation" is carried out using a **guardianship credential**. It acts much like the digital equivalent of a guardianship order from a court (and in fact may be authorized by such an order). It enables the guardian to set up and operate an SSI agent and wallet on behalf of the dependent and, when necessary, prove that they are acting in the capacity of a guardian. This extends the benefits of SSI to literally any person regardless of physical, mental, or financial capacity.

4.2.5 Payment and value exchange

Mention the phrase "digital wallet" and the first thought that will comes to many people's minds is payments—because that's the primary task for which we use our physical wallets today. If digital wallets are the core metaphor for SSI, people are going to expect them to be used for payment in addition to identity.

Figure 4.2: Digital wallets are the core metaphor for SSI—so it feels natural that they would be applied to payments.

Indeed, since SSI digital wallets incorporate everything necessary for the trusted exchange of digital information—DIDs, private connections, private keys, agent endpoints—then extending them to the safe exchange of digital payments is very natural. The good news is:

1. From the standpoint of SSI agents, payments are just another type of workflow.
2. SSI wallets can be designed to work with any type of currency (including cryptocurrencies), payment system, or payment network (including credit/debit card networks).
3. With digital wallets and verifiable credentials, payment can be integrated directly into workflows that require KYC and AML as discussed above.

Even better news: **payments are just one type of value exchange than can be automated using SSI**. The term "payment" usually means a specific type of currency—fiat currencies like dollars, pounds, euros, yen, or cryptocurrencies like bitcoin and ether. However there are many other means of value storage and exchange beyond those: points, airline miles, coupons, and many other different types of loyalty programs. And SSI digital wallets and agents can be used for all of them as fast as these value exchange systems can be translated to verifiable credentials and agent-to-agent protocols. (See the Scorecard entry for *Loyalty and reward programs* later in this chapter.)

This in turn means payments can be integrated into almost any business process workflow at almost any level of assurance and regulatory compliance. Payment automation is the frosting on the SSI-enabled BPA cake.

4.3 Feature/benefit category #3: user experience & convenience

This category will look at the same five features and benefits as the last category (business efficiencies), but this time through the lens of how they benefit the end-user.

4.3.1 Auto-authentication

How much do users hate passwords? A July 2019 study by MobileIon reported in Security InfoCenter[101] said that when users encounter password troubles:

- 68% feel disrupted
- 63% feel irritated and frustrated
- 62% feel they have wasted time.

The same study found that:

- IT security leaders felt they could reduce their risk of breach by almost half (43%) by eliminating passwords.
- 86% of those security leaders would do away with passwords if they could.
- 88% of these leaders believed that in the near future, mobile devices will serve as your digital ID to access enterprise services and data.

In February 2019, user-centric biometric authentication leader Veridium published a study of more than 1000 U.S. adults who have experience with biometrics (such as Apple's TouchID or FaceID) found that 70 percent wanted to expand their use into everyday login.[102] Speed (35 percent), security (31 percent), and not having to remember passwords (33 percent) were cited as the primary incentives.

On May 1, 2018, Microsoft announced in a blog post that it was "Building a world without passwords".[103] To quote:

> *Nobody likes passwords. They are inconvenient, insecure, and expensive. In fact, we dislike them so much that we've been busy at work trying to create a world without them – a world without passwords.*

[101] https://www.securitymagazine.com/articles/90530-in-10-it-leaders-want-to-eliminate-passwords
[102] https://www.businesswire.com/news/home/20190213005176/en/Veridium-Survey-Reveals-Strong-Consumer-Sentiment-Biometric
[103] https://cloudblogs.microsoft.com/microsoftsecure/2018/05/01/building-a-world-without-passwords/

This is why Microsoft has been a major supporter of DIDs—the decentralized identifiers at the core of SSI—and are building DID-based passwordless authentication into multiple products.[104]

In short, the age of the password is about to pass, and for users everywhere it could not come fast enough. There will be rejoicing in the streets.

4.3.2 Auto-authorization

If passwordless auto-authentication will replace the login screen, **auto-authorization will replace many (but not all) Web forms**. Can you hear more rejoicing?

Here are some realities about online forms:

- 81% of people have abandoned a form after beginning to fill it out.[105]
- 29% of people cite security reasons as one of their main concerns when it comes to completing online forms.[106]
- More than 67% of site visitors will abandon your form forever if they encounter any complications; only 20% will follow up with the company in some way.[107]
- 23% of people will not fill out your checkout form if you require them to create a user account.[108]
- Better checkout design can reduce form abandonment by as much as 35%, which translates into nearly $260 billion in recovered orders.[109]

When you stop to think about it, SSI auto-authorization solves almost every typical complaint about online forms:

- **There is no typing.** All the information being requested by the verifier is being transferred from claims to your digital wallet. And even if new self-attested data is requested, your agent can capture it for you so you'll never have to type it again.
- **Your connection is your account.** The whole idea of "click here to automatically create an account with this form data" goes away. You automatically have an "account" anywhere you have a connection.
- **Data verification is built-in.** The main point of verifiable credentials is that the claims data has already been vetted by the issuer.
- **Security is built-in.** All proofs and data sent by your SSI agent automatically use your encrypted private connection with the verifier.
- **Privacy and selective disclosure are built-in.** First, verifiers can now ask only for

[104] https://www.microsoft.com/en-us/security/technology/own-your-identity
[105] https://themanifest.com/web-design/6-steps-avoiding-online-form-abandonment
[106] https://wpforms.com/online-form-statistics-facts/
[107] https://wpforms.com/online-form-statistics-facts/
[108] https://wpforms.com/online-form-statistics-facts/
[109] https://wpforms.com/online-form-statistics-facts/

the minimum information they need—reducing their potential liability. Secondly, the proof your agent sends can be read only by the verifier. If the verifier needs a copy of the underlying data (e.g., asks you to share your actual birthdate instead of just proving you are over 18), your agent should be able to automatically warn you if that data will not covered by a satisfactory privacy policy or governance framework.

- **Auditing is built-in.** Your agent can automatically track all the information you share—without requiring you to share that history with anyone else.

In addition, verifiable credentials let you prove many more things about yourself—as an individual, a student, an employee, a volunteer, or in any other role you play—than you could prove via any Web form today. With auto-authorization, **your ability to perform tasks online comes much closer to your ability to perform those same tasks in the real world**—i.e., using your physical wallet, paper credentials, and face-to-face verification—but orders of magnitude faster.

4.3.3 Workflow automation

From the standpoint of the end-user, SSI has the potential to reduce workflow steps that currently can take hours or days to as little as a few buttons on a smartphone. One such scenario—the selling of a car and the transfer of the title and registration from one owner to another—was described in detail in the final scenario in chapter 3.

Many more of these scenarios are covered in detail in Part 4, where we examine the impact of SSI across eight different industries and market verticals. You will see the same patterns repeated over and over: a business process carried out, step by step, by employees, contractors, suppliers, regulators, and other participants exchanging verifiable credentials (or digitally signed messages authorized by these credentials) between their agents and wallets. For every step, all of the following are performed automatically for the user:

1. **Authentication** that the user is the correct party.
2. **Authorization** that the user has the authority.
3. **Verification** that the step is being performed in the right sequence of the business process (and that its preconditions have been met).
4. **Validation** that the claims or messages meet the requirements of the business process.
5. **Routing** of the credential or message produced to the next agent or agents needed in the process.
6. **Logging** of the action taken to provide a full digitally-signed audit trail (or even automated reporting to regulators—see the very last section of this chapter).

Perhaps the ultimate example of consumers experiencing the convenience of SSI-enabled workflow automation is the perennial **change-of-address** problem. An individual is moving house and needs to inform dozens if not hundreds of agencies, suppliers, and contacts about the new address. Despite the advent of the Internet and the Web, this is still an excruciatingly labor intensive process for the individual. The main reason? **Account takeover.**[110] Fraudulent change-of-address is the first step in hijacking a bank account, credit card account, company account, or other valuable account in order to steal from it—or use that account to steal from others. So companies need to add extra hoops to ensure it's really you requesting a change-of-address.

With SSI and verifiable credentials, change-of-address can be performed in three easy steps:

1. Obtain a verifiable credential of your new address from a widely trusted issuer.
2. Send a proof of that credential over all your connections who need to know your new address.
3. **Each of their back-end systems can verify the proof** and update their systems with your new address with high confidence that it is valid.

Voila. Tens of hours of human labor and hundreds of dollars in business savings for every single change-of-address notification. Given that in America alone an average of 35 million people move house every year,[111] this alone adds up to **hundreds of millions of man-hours and hundreds of billions of dollars in savings every year**.

4.3.4 Delegation and guardianship

As we described above, delegation credentials are what enable much of this workflow automation magic. Thankfully, the process of obtaining (or assigning) delegation credentials is just another workflow. The delegator first establishes a connection with the delegate (or vice versa) and then issues a credential granting the necessary authorizations.

Delegation credentials can be revised or revoked as conditions and positions change, with both the requirements and the current status being maintained by orchestration agents. All of this can be set forth in one or more governance frameworks that define the legal and business rules applying to the entire business process, whether it is taking place entirely inside one company, across a supply chain, across an entire industry, or in a wide-open process such as international shipping that crosses multiple industries and government jurisdictions. As a general rule, if humans can define the rules of the process, including who can make what decisions when, then SSI agents, wallets, and verifiable credentials can be used to automate the necessary information exchanges.

---

[110] https://en.wikipedia.org/wiki/Credit_card_fraud#Account_takeover
[111] https://www.move.org/moving-stats-facts/

The end result is that so many of today's most difficult user experience challenges— especially entering or interpreting data presented by machines—can be simplified by being able to focus just on the analysis and decisions that humans really need to make.

4.3.5 Payment and value exchange

For decades the challenge of moving money safely has the focus of entire industries—banking, credit unions, credit cards, and now cryptocurrencies. It is the very heart of human economic activity. And, like the human heart, it is the most vulnerable to attackers. As Willie Sutton famously answered when asked why he robbed banks, "Because that's where the money is."[112]

So there has always been a tension between making it easier to move money and making it safe to do so. Every means of value transfer from Pony Express to Paypal has spawned a new legion of criminals to exploit it. Cryptocurrencies—arguably the most friction-free way to move money ever invented—are no different. Coindesk reported that in the first nine months of 2018, nearly $1 billion had been stolen from cryptocurrency exchanges and other crypto holders.[113]

While SSI is not a panacea, it does provide a complete infrastructure for trusted information exchange. This includes payments and other forms of value exchange as discussed above. With all of the protections that SSI digital agents, wallets, connections, and verifiable credentials provide, SSI could be the infrastructure that finally—from the perspective of end-user experience—makes digital payments one-click easy AND secure at the same time.

The effect on digital commerce can be profound. Amazon's one-click purchasing capability famously helped vault it to the forefront of ecommerce. With the expiration of Amazon's one-click patent[114] and the arrival of SSI payments infrastructure, a feature that once exclusively belonged to Amazon could now become "**one click everywhere**".

4.4 Feature/benefit category #4: relationship management

While saving time and money is important, there is another category of features and benefits that is not purely monetary: those that increase the trust, productivity, and value of relationships.

Customer relationship management (CRM) is already a dominant industry in its own right. In January 2019 Forbes reported that:[115]

- **CRM now makes up nearly 25% of the entire enterprise software revenue market.**

---

[112] https://en.wikipedia.org/wiki/Willie_Sutton
[113] https://www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research
[114] https://digiday.com/marketing/end-era-amazons-one-click-buying-patent-finally-expires/
[115] https://www.forbes.com/sites/louiscolumbus/2019/06/22/salesforce-now-has-over-19-of-the-crm-market/

- Worldwide spending on CRM software grew 15.6% to reach $48.2B in 2018.
- Salesforce is the leader, with 19.5% of the CRM market, followed by SAP at 8.3%).

The impact of SSI on CRM has long been anticipated by a movement known as **vendor relationship management (VRM)**. Its leader, Doc Searls, pithily summarizes it as "the inverse of CRM", i.e., VRM how people can control their relationships with companies. For details see _____, the chapter Doc has contributed to this book.

Without stealing Doc's thunder, this section will examine five key ways that SSI will enable better relationship management in both directions.

4.4.1 Mutual authentication

The first place SSI can improve relationships is right at the very start. This is when the parties are most vulnerable—when they are meeting each other for the first time, especially digitally.

On the web today, this is a struggle from both sides. First, imagine how hard it is for a website to prove that is authentic when **phishing sites** and **phishing emails** have become so good that even trained professionals can have a hard time spotting them.[116] Verizon's 2018 Data Breach Incident Report said phishing accounted for 93% of all data breaches.[117] Between October 2013 and May 2018, the U.S. Federal Bureau of Investigation (FBI) reported $12.5 billion in losses to companies due to phishing.[118]

Now turn the tables and think about how hard it is for **you**, the end-user, to prove to a website that *anything* about yourself is authentic. Most of us have a hard time even proving we are **human**. How many of us have tripped up over one of these?

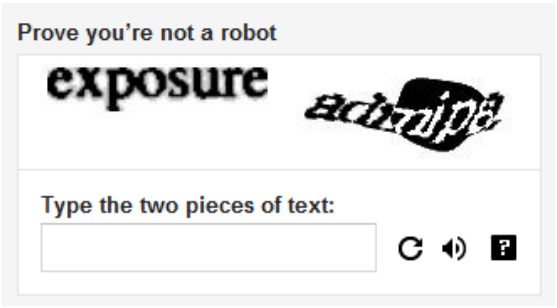

Figure 4.3: A CAPTCHA (completely automated public Turing test to tell computers and humans apart) can often be hard for even a real human to pass.

[116] During the writing of this book, one of the co-authors received an email from his bank (a household brand) that was so realistic, it took three phone calls to determine is was a phishing attempt.
[117] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
[118] https://www.ic3.gov/media/2018/180712.aspx

If it's that hard to prove you are even human, how are you supposed to prove:

- You are over or under a certain age
- You live in a certain place
- You have a certain degree
- You have a certain job
- You have a certain income

Generally these tasks are impossible over the Internet without: a) proving your real-world identity to the website (somehow), and then b) having the website independently verify information about you from some authoritative source (like a credit rating agency)—or worse, some data broker who may or may not have accurate information about you (let alone permission from you to share it).

This problem has become acute in both directions—**and SSI can solve it in both directions**. The beauty of SSI auto-authentication (see the earlier sections) is that your agent can not only share verifiable credentials with a website, but the website's agent can share verifiable credentials with you. Both agents can automatically verify the credentials on behalf of their owners to make sure they meet their respective policies. If so, the relationship can proceed without a hitch. If either agent spots a problem, it can immediately flag its owner—or simply deny the connection, so its owner is never bothered.

This is how all our digital relationships should work—mutual auto-authentication on both sides that will put phishers permanently out to sea.

4.4.2 Permanent connections

The second major benefit SSI brings to relationship management is a feature no network has ever offered before: **permanent connections**. By permanent, we mean a connection that can last literally *forever* if both parties want it to.[119]

How can SSI make such a promise? No other digital connection—a phone number, an email address, a Twitter handle, a Facebook friend, a LinkedIn connection—can make that promise. Why? **They all depend on some form of intermediary service provider for the connection to keep working**. And no intermediary service provider can promise to always be in business and always maintain your connections no matter what you do or what your connections do.

In fact, most of them promise you *the exact opposite*: they can terminate your service at any time, for any reason. Just read your terms of service.

With SSI—and the decentralized networks that make it work—there is no intermediary service provider. **Your connections belong to you.** You—or the other party—are the only ones who can terminate a connection because one or both of you want to end the relationship.

---

[119] The mathematical techniques used to generate DIDs produce numbers so large that, even after thousands of years, the chances of generating the same ones are infinitesimally small.

How valuable is this to you—the individual who wants to stay in touch with the people, organizations, and businesses in your life when you move, change jobs, graduate from school, or change service providers? And how valuable is it to all of your contacts and vendors who are trying to keep track of you? Earlier in this chapter we quantified that simply automating change-of-address could save millions of hours and billions of dollars annually. Multiply that by all the other information we'd like to keep "in sync" with each other over permanent connections , and the total savings could be an order of magnitude greater.

4.4.3 Premium private channels

Permanence is not the only benefit of SSI connections. Because they are based on DIDs, DID documents (with public keys) and the DIDComm protocol that we explain in part 2 of this book, all of them natively support **end-to-end secure encrypted communications**.

From a marketing perspective, we call these **premium private channels**. "Premium" because they are exclusive to you and your connection—they are not shared by anyone else. "Private" because all your communications are automatically encrypted and decrypted by your respective agents without any effort on your part. "Channels" because you can use them to send and receive any messages or content your respective agents can "speak".

So your connections can be used—without any permission from anyone else—with any SSI-enabled application: messaging apps, voice and video apps, data sharing apps, social networking apps, productivity apps, payment apps, games, and so on. Every one of these apps can have access to every SSI feature described in this chapter.

Messaging apps have been moving in this direction for some time. Apple iMessage, WhatsApp, Signal, and Telegram all support end-to-end encryption in one form or another. Others, like WeChat and Alipay in China, have also integrated messaging with secure payment and so many other plug-in functions such that many Chinese spend their entire day living and working in these apps.[120]

SSI makes premium private channels a universal capability that can be integrated with any app and that can work across any trust boundary—just like the Internet and the Web. You will find multiple examples in Part 2 of this book. For instance, CULedger, a global consortia of credit unions developing SSI infrastructure for the credit union industry, plans to use premium private channels to request secure, digitally-signed authorizations and consents from credit union members for actions that would otherwise require members to send a fax or make an in-person visit to a credit union office.

4.4.4 Reputation management

Reputation systems have become an essential feature of doing business on the Web. For example, a Spiegel Research Center study showed nearly 95% of shoppers read online

[120] https://medium.com/@wechatminiprogrammer/alipay-vs-wechat-pay-an-unbiased-comparison

reviews before making a purchase.[121] A 2016 Harvard Business School study said a one star increase on Yelp can lead to a 5-9% increase in revenue for a merchant.[122]

However it is precisely because they are so valuable that attacking reputation systems has become big business. A February 2019 study from Fakespot, which analyzes customer reviews, revealed that 30% of reviews on Amazon are fake or unreliable, and a whopping 52% of reviews posted on Walmart.com are inauthentic.[123] Worse, the rise in fake reviews is undermining consumer confidence in reputation systems. A Bright Local 2018 study said 33% of all consumers reported spotting "lots" of fake reviews, and that the number went up to 89% for 18-to-34-year-olds who are savvier at detecting the signs of a fake review.

Amazon has long tried to fight this gaming with various protection measures, including its **Amazon Verifier Purchase** program that is supposed to ensure the reviewer actually bought the product.

Figure 4.4: An Amazon Verified Purchase marking is supposed to confirm that the reviewer bought the reviewed product—but they are not difficult to work around.

However this only works if a reviewer actually purchased the product at Amazon, and even then, it is relatively easy for a savvy marketing company to subsidize these purchases or find other ways around Amazon's rules. And if Amazon has these issues, imagine the scope of the problem for smaller sites that have only a tiny fraction of Amazon's security budget.

At this point in the book it should be obvious how SSI can help with this problem. First, reputation systems can require verifiable credentials for reviewers, weeding out the bots. Second, they can require a verifiable credential for a product purchase—a **verifiable receipt**—so programs like Amazon Verifier Purchase can can work independently of any particular retailer. Thirdly, reviewers can actually start to build reliable reputation independent of not just any product vendor but of any retailer—so we can start developing an ecosystem of widely trusted independent reviewers that can become the Web equivalent of, say, Walter Mossberg of the Wall Street Journal or Jon Udell in his days at Byte Magazine.

---

[121] http://spiegel.medill.northwestern.edu/online-reviews/
[122] https://www.hbs.edu/faculty/Pages/item.aspx?num=41233
[123] https://www.cbsnews.com/news/buyer-beware-a-scourge-of-fake-online-reviews-is-hitting-amazon-walmart-and-other-major-retailers/

In short, **reputation management can become an integral part of relationship management**. Any two parties that develop a connection and engage in interactions with each other—purchases, contracts, consulting, or just community engagement—should be able to provide verifiable reputational feedback to each other and to the larger community.

The implications extend to any online survey, poll, or vote where it matters that: a) real human beings and not bots are participating, b) each unique person has only one vote, and c) people need to be accountable for voting honestly and not trying to game the system. Gaming these types of systems with fake votes has become such a common attack that the security community gave it the name **Sybil attack** after the famed case of multiple- personality disorder that was the subject of a 1973 book and a 1976 movie.[124]

As fake reviews, fake sites, and fake news multiple like rabbits on online, the ability for SSI to counter Sybil attacks and anchor the trustworthiness of reputations systems may become one of its most valuable contributions to the future health of the Web.

4.4.5 Loyalty and rewards programs

Every relationship involves an exchange of value of some kind between the two parties—even if it's just an exchange of pleasantries among neighbors. If that exchange is monetary, our earlier discussions of how SSI enables new forms of payment apply. But the stronger a relationship grows, the higher the probability it involves some form of non-monetary value exchange.

Rewards programs are a perfect example. Whether they involve miles, points, stamps, or some other measure of value, they are an informal, direct, relationship-based way of thanking a customer for past loyalty and incentive future loyalty. And they work:

- 69% of consumers say choice of retailer is influenced by where they can earn customer loyalty/rewards program points.[125]
- A 5% increase in customer loyalty will increase the average profit per customer by 25-100%.[126]
- 76% of consumers think that loyalty programs are part of their relationship with brands.[127]
- The Loyalty Management market is expected to grow from $1.4 billion in 2015 to $4.0 billion by 2020.[128]

However for consumers today, managing loyalty programs is anywhere from mildly inconvenient to downright irritating. Imagine if every retailer you dealt with required you to

[124] https://en.wikipedia.org/wiki/Sybil_attack
[125] http://www.prweb.com/releases/2013/11/prweb11372040.htm
[126] http://en.wikipedia.org/wiki/Loyalty_Effect
[127] https://www.invespcro.com/blog/customer-loyalty-programs/
[128] http://www.prnewswire.com/news-releases/loyalty-management-market-worth-usd-40-billion-by-2020-545897032.html

not only use a different type of money, but **a different wallet**—one dedicated to their specific store. That would be ridiculous—yet that is how loyalty programs work today.

SSI-based relationship management (also called vendor relationship management or VRM as noted above) can turn that on its head. Now every loyalty program can be designed to use its own premium private channel **to the consumer's own SSI digital wallet**. No matter what kind of loyalty currency is involved, they can all be managed securely and privately in one place. Consumers gain dramatically greater convenience and control; retailers gain simpler and more effective loyalty programs that can also take advantage of all the other features of SSI.

4.5 Feature/benefit category #5: Regulatory compliance

Our final category may be the least "sexy" but in some ways the most significant because it covers how SSI can contribute to the strength of our global cybersecurity and cyberprivacy infrastructure. In this section we'll cover five major ways SSI can help all actors in the global economy comply with regulations designed to keep us safe while at the same time encouraging greater economic activity through open and fair competition.

4.5.1 Data security

We could begin this section with a shower of statistics about the state of security on the Internet, but they are all summed up by this 2015 quote in Forbes from Gina Rommety, CEO of IBM, when she addressed the CISOs (Chief Information Security Officers), CIOs, and CEOs of 123 companies in 24 industries:[129]

> *"We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."*

That same Forbes article said market estimates of the size of the worldwide cybersecurity industry range from $77 billion in 2015 to $170 billion by 2020. It is one of the fastest growing of all enterprise software segments.

By attacking the very root of the problem—digital identity—SSI represents a sea-change in cybersecurity. SSI agents will help users generate and manage private keys, automatically negotiate pairwise pseudonymous DIDs, form secure connections, and communicate over premium private channels that provide the data security required by regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation) in Europe. This alone will lock down acres of current

[129] https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/

vulnerabilities—one reason the U.S. Department of Homeland Security funded much of the research into the decentralized identifier[130] and decentralized key management[131] standards that are the foundation of SSI.

SSI can also "detoxify" personal data so it can no longer be used for identity theft and related cybercrimes. Today this personal data is valuable because if a thief has enough of it, he/she can impersonate you to either break into current accounts or open new accounts in your name. But with verifiable credentials, **your personal data alone can no longer be used to steal your identity**. If the thief does not have your private keys, he/she cannot produce proofs of your verifiable credentials.

This means **breaches of huge corporate databases containing personal data will become a thing of the past.** Unlike usernames, passwords, and other personal data today, your private keys will never be stored in some centralized corporate database that serves as a giant honeypot[132] for criminals. They are always stored in your local devices, with an encrypted backup copy in the cloud (or wherever you direct it to go). This means that to steal an identity, a thief has to break into your personal SSI wallet(s), one at a time.

This is like forcing criminals to eat by catching tiny minnows one at a time instead of spearing a whale. Give criminals that choice and they will find another way to eat.

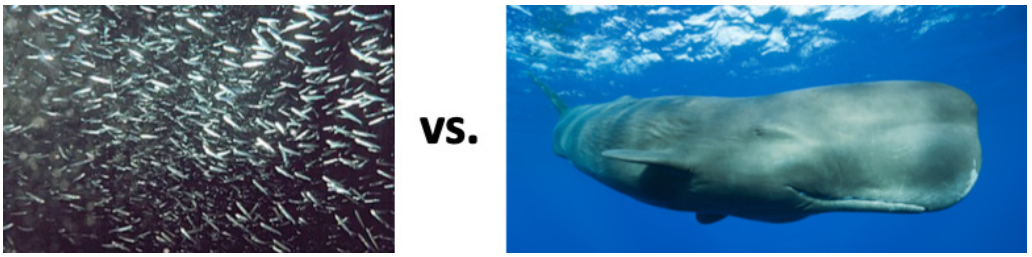

Figure 4.5: SSI will force identity thieves to try to steal private keys one wallet at a time (left) vs. break into giant corporate honeypots of personal data (right).

4.5.2 Data privacy

Security and privacy go hand in hand, and privacy is every bit as much of a concern on the Internet today. In June 2018 Entrepreneur Magazine reported 90% of Internet users were "very concerned" about Internet privacy.[133] The same article reported that the Cambridge Analytic data scandal[134] so tarnished Facebook's reputation that only 3% of users trust how Facebook is handling their personal data (and only 4% trust Google).

---

[130] https://www.sbir.gov/sbirsearch/detail/867797
[131] https://www.dhs.gov/science-and-technology/news/2017/07/20/news-release-dhs-st-awards-749k-evernym-decentralized-key
[132] https://en.wikipedia.org/wiki/Honeypot_(computing)
[133] https://www.entrepreneur.com/article/314524
[134] https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

Part of what has pushed Internet privacy to this crisis level is the sheer economic value of personal data in today's digital economy. In an April 2019 review of Shoshana Zuboff's book *The Age of Surveillance Capitalism*,[135] The Nation magazine said:[136]

> **Zuboff shows that these increasingly frequent invasions of our privacy are neither accidental nor optional; instead, they're a key source of profit for many of the 21st century's most successful companies. Thus, these companies have a direct financial stake in the broadening, deepening, and perfecting of the surveillance they already profit from—and in making sure that it remains legal.**

Shifting the balance of power in privacy and personal data control will not be easy. However, SSI can help companies comply with applicable privacy legislation in three specific ways:

1. **Selective disclosure.** SSI verifiable credential exchange technology—specifically for credentials that use zero-knowledge proof cryptography—enables companies to request proofs of exactly the personal data they need and no more. For example, a company can request proof you are over a specific age, rather than your actual birthdate.
2. **Verifiable consent.** Many consumers have no idea where companies get their personal data. Did it come from online forms they filled out? From marketing partners? From third party data brokers? With verifiable credentials, there is a clear, verifiable chain-of-consent to share data that starts with the individual and can easily be traced and audited by the responsible SSI agents.
3. **Governance frameworks.** Today, most privacy policies are highly custom documents written by lawyers to protect specific companies—not your privacy. Which is why ten years ago a study by privacy researchers Lorrie Faith Cranor and Aleecia McDonald estimated **the average person would require 76 work days** to read the privacy policies on the websites they visit, which for the United States alone would add up to **53.8 billion hours** or **$781 billion in labor costs**.[137] With SSI, company-specific privacy policies could begin to be replaced by governance frameworks that: a) are uniform across all the sites that adopt them, b) can be developed in open public forums to represent the best interests of all stakeholders, c) can be pre-approved by regulators to comply with their requirements, and d) can be designed to incorporate the other protections and advantages of SSI.

These steps could become the first Internet-scale implementation of the principles of *Privacy by Design* as developed and advocated by former Ontario Information and Privacy Commissioner Ann Cavoukian.[138]

---

[135] https://www.shoshanazuboff.com/new/the-age-of-surveillance-capitalism-comments-and-reviews/
[136] https://www.thenation.com/article/shoshana-zuboff-age-of-surveillance-capitalism-book-review/
[137] https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/
[138] https://en.wikipedia.org/wiki/Privacy_by_design

4.5.3 Data protection

Although closely related to data privacy, data protection goes beyond privacy controls to enumerate a larger set of specific principles for the protection of an individual's personal data. Although the European Union's General Data Protection Regulation (GDPR)[139] is the best known data protection legislation, it is by no means the only one. The California Consumer Privacy Act (CCPA)[140] is setting a new standard for data protection regulation in the U.S., and many other countries have or are enacting data protection laws along the same lines.

In addition to the data privacy compliance mechanisms listed the previous section, there are other very specific ways that SSI can enable both individuals to exercise their rights and companies to comply with their responsibilities under these data protection acts. To wit:

1. **Pseudonymous identifiers.** GDPR encourages the use of pseudonyms to minimize correlation. SSI connections use pairwise pseudonymous peer DIDs by default.
2. **Data minimization.** GDPR requires collecting no more personal data that is necessary for the purpose for which it is being processed. SSI selective disclosure and ZKP credentials are ideal for meeting this requirement.
3. **Data accuracy.** GDPR requires that personal data must be accurate and kept up to date. SSI enables data controllers to request personal data supplied by verifiable credentials from reputable issuers—and which can be automatically updated by those issuers when the data changes.
4. **Right of erasure** (also known as the "right to be forgotten"). Enshrined by Article 17 of GDPR, this can be one of the most challenging requirements because it means the data controller (the company) must give the data subject (the individual) a means of confirming what personal data a company holds while at the same time not opening a security hole for attackers. Thankfully this is precisely the job that SSI connections and premium private channels were designed for. The data subject can use auto-authentication and auto-authorization to request access to the data, and if desired send a digitally-signed request for erasure over the connection. All of these actions can be securely audited for later verification of compliance.

4.5.4 Data portability

GDPR enforces one more data protection right that is deserving of its own discussion: data portability. This is the right that allows data subjects to obtain data that a data controller holds on them and reuse it for their own purposes. It the words of the first paragraph of Article 20 of the GDPR:

---

[139] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[140] https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

> *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided…*

GDPR is only one of many new regulations requiring partial or complete data portability across data controllers. And other regulation from the European Union as the second Payment Services Directive (PSD2) which aims to drive open banking in the EU[141], the Fifth Anti-Money Laundering Directive (AML5)[142] and Electronic Identification, Authentication and Trust Services (eIDAS)[143] or the Directive on Security of Network and Information Systems (NIS Directive)[144] might all impact SSI implementations. All of these were preceded by the requirement for local telephone number portability (LNP) in the U.S. Telecommunications Act of 1996, which in the U.S. also applies to mobile number portability (MNP). MNP is also required to varying degrees by legislation in Africa, Asia, Australia, Latin America, and Canada.

SSI is ideal for data portability because it solves so many of the deep security and privacy issues as described in the previous sections. The secret is that SSI connections make it easy for the data **to flow in and out of connections with the individual data subject's own agent**, where the individual can always exert complete control over the data and the terms and conditions under which he/she is willing to share it with other parties.

Under this architecture—and especially under governance frameworks designed specifically to work with this architecture—personal data should be able to flow freely between systems while meeting the security, privacy, and control requirements of GDPR and other data protection regulations.

4.5.5 RegTech (Regulation Technology)

As substantial as all these breakthroughs are, the one regulators may get most excited about is the ability to connect directly to SSI ecosystems *themselves*. In other words, by deploying their own SSI agents and connecting directly to the companies being regulated, **regulators can be directly "in the loop" of transactions with specific regulatory requirements**—such as KYC requirements for opening a bank account, AML requirements for money transmission, or ATF requirements for purchases of certain types of goods.

For example, if a money transmission between two SSI-enabled parties exceeds the threshold over which a financial institution must apply additional AML compliance measures, this can be communicated in real time between the bank's SSI agent and the regulator's SSI agent. This has the potential to change the very nature of regulation enforcement from **an**

---

[141] https://en.wikipedia.org/wiki/Payment_Services_Directive
[142] https://www.electronicid.eu/aml5-new-anti-money-laundering-directive/
[143] https://en.wikipedia.org/wiki/EIDAS
[144] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

after-the-fact spot-check auditing activity to a real-time rules-driven monitoring activity—decreasing enforcement costs, speeding up enforcement actions, and improving the quality of enforcement data all at the same time—a rare triple win for government.

This is a highly desirable development given the skyrocketing costs of compliance cited earlier in this chapter. It is also consistent with the rapid growth of the global Regulatory technology (RegTech)[145] market, which Research and Markets expects to grow from USD 4.3 billion in 2018 to USD 12.3 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 23.5%.[146] With the ability of SSI technology to connect secure, private, permissioned SSI agents to any business process requiring regulation, that growth figure could be much higher.

4.6 Using the SSI Scorecard in Part Four

In this chapter we have:

- Introduced a scorecard of 25 major features and benefits of SSI divided into five major categories.
- Defined each category and described the five most important features and benefits within it.
- Provided evidence of the market impact of each of these key features and benefits and shown how many of them are interrelated.

As its name indicates, the SSI Scorecard is a tool for analyzing the impact of SSI on any particular use case, application, industry, or vertical market. We will do just that in Part Four of this book, where we will examine in-depth use cases for SSI across eight vertical markets. Each chapter will wrap up with a scorecard for how much impact SSI is likely to have in that market along and why. This should help tie together the building blocks, example scenarios, and features/benefits we have covered in Part One with the real-world scenarios we are going to be looking at in Part Four.

If you are interested in reading directly more about the impact in business and different verticals we recommend you to jump directly to Part Five of the book. If you are more of a technical mind and wanted to deep dive into the building blocks just turn the page and start reading from some of the leading experts in the world of each of those building blocks how they make SSI possible in in Part Two and Three

[145] https://en.wikipedia.org/wiki/Regulatory_technology
[146] https://www.researchandmarkets.com/research/r8ktnm/global_12_3?w=5