FOM Hochschule für Oekonomie & Management

Hochschulzentrum Düsseldorf

Project Paper

part-time degree program

6. Semester

in the study course Wirtschaftsinformatik (B. Sc.)

as part of the course

Web & Social Media Analytics

on the subject

Sign in with Google - Opportunities and risks of using single sign-on providers for managing user accounts on websites

by

Luis Pflamminger

Advisor:	Prof. Dr. Carolin Tewes
Matriculation Number:	538276
Submission:	22. August 2022
Word Count:	4377

Abstract

Internet users today have to remember passwords for many different websites. Website owners on the other hand want to give users the option to create an account and log in as seamlessly as possible, while also obtaining the required user data. A modern solution to this problem on the web is Single Sign-On (SSO). This paper gives an understanding of how the technology works by explaining basic concepts and giving an overview of protocols and SSO providers. Furthermore, it discusses opportunities that SSO offers for online service providers and examines associated risks.

Contents

List of Figures

List of Tables

List of Abbreviations

SSO	Single Sign-On
SMS	Short Message Service
SFA	Single-Factor Authentication
2FA	Two-Factor Authentication
MFA	Multi-Factor Authentication
API	Application Programming Interface
IdP	Identity Provider
SP	Service Provider
RP	Relying Party
FIM	Federated Identity Management
SAML	Security Assertion Markup Language
NIST	National Institute of Standards and Technology
US	United States of America
XML	Extensible Markup Language

1 Introduction

1.1 Motivation

The web is a big part of most people's lives. Social media services are used to keep in touch with friends and family, discover new things and keep up to date with ones individual interests. Streaming services and video platforms are used to consume content, e-commerce sites are used for shopping and online productivity suites are used constantly in the workplace in a wide range of industries.

Most modern web services require users to create an account so the platform can keep track of user data and provide personal recommendations. This results in the average user having around 36 unique login combinations they need to remember[1], which leads to many users forgetting their password or re-using passwords on multiple sites.

There are many solutions to this problem, such as password managers or auto-fill features in modern web browsers. A different solution that doesn't rely on password management on the user's side is called Single Sign-On (SSO). It allows users to log into many different web services using a single set of credentials[2]. Large internet corporations like Google and Facebook provide services that allow users to sign into different websites using their existing account[3]. Websites get the benefit of providing users with a quick way to sign in, simplifying their user interfaces and getting access to existing user data[4]. This paper examines how SSO works, what opportunities it provides and which risks are associated with implementing it.

1.2 Research Goals & Structure

This paper's structure is tightly aligned with its goals.

The first goal is to give an understanding of how SSO functionality works. To achieve this, the basics of authentication and authorization are explained in section 2.1.1. Next, important terms related to SSO are defined and the types and use cases, as well as protocols and technologies are examined (section 2.2). Then an overview of SSO providers is given.

[1] Cp. *Florencio*, *D.*, *Herley*, *C.*, Password Habits, 2006, p. 4.
[2] Cp. *Radha*, *V.*, *Reddy*, *D. H.*, Survey SSO Techniques, 2012, p. 134.
[3] Cp. *Gafni*, *R.*, *Nissim*, *D.*, Factors Affecting Social Login, 2014, p. 2.
[4] Cp. *Google*, Sign In With Google, 2022.

The second goal is to present opportunities that SSO gives businesses that operate websites and platforms targeting end users on the open web. To achieve this, important opportunities are explained and discussed in section 3.

The third goal is to present and discuss some of the risks that come with implementing SSO from the point of view of a business operating a website (section 4).

Finally, the paper is concluded and possible shortcomings are discussed.

2 Fundamentals of Single Sign-On

2.1 Basics of Authentication

2.1.1 Authentication & Authorization

Authentication is the act of establishing a user's identity. The user has to prove, that they are who they say they are[5]. There are three main ways how a user can prove their identity:

1. The user provides some secret, that only they know, e.g. a password.
2. The user provides something, that only they have. An example for this is a Short Message Service (SMS) based authentication system, where the user receives a message containing a code, which has to be entered into the login form. They thus prove, that they are in possession of the phone with the phone number they have previously provided.
3. The user proves their identity by using some unique physical characteristic, e.g. a fingerprint or eye retina scan.[6]

Using only one of these ways to authenticate a user is called Single-Factor Authentication (SFA), using two is called Two-Factor Authentication (2FA) and using multiple factors is called Multi-Factor Authentication (MFA). Using two or more factors for authentication improves security and is deemed essential for applications with sensitive data.[7]

Contrary to authentication, authorization determines whether a user is allowed to access a specific resource. It happens once the user has been authenticated.[8] For example, user *A* might make a post on a social media site which is only shared with their close friends. If user *B* wants to view the post, the system first checks if user *B* is part of user *A*'s close friends. If they are, they are authorized to see the resource.

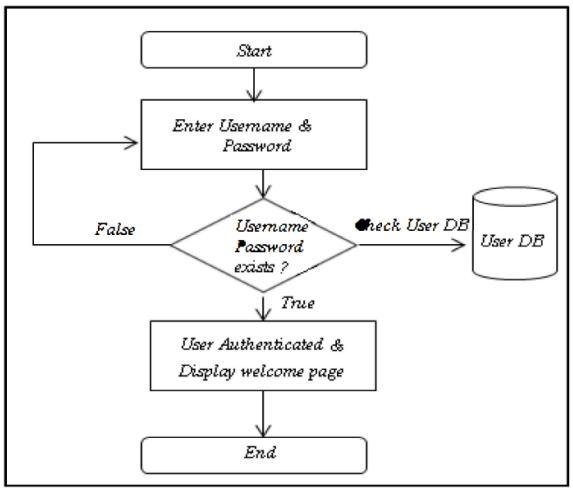
2.1.2 Authentication flows without SSO

Figure 1 shows a flow chart for a traditional authentication flow using a username and password. The user enters their information and clicks the "Sign In" button. Next, the

[5] Cp. *Basavala*, *S. R.*, *Kumar*, *N.*, *Agarrwal*, *A.*, Authentication Overview, 2012, p. 398.
[6] Cp. ibid., p. 398.
[7] Cp. *Drew*, *J.*, 2FA Mandatory, 2019.
[8] Cp. *Auth0 Inc.*, AuthN vs. AuthZ, n. d.

server checks in a database whether or not the username exists and if the password is correct. If this is true, the user is authenticated and is allowed to enter the website.[9]

Figure 1: Flow chart of an SFA authentication process



Source: *Basavala*, *S. R.*, *Kumar*, *N.*, *Agarrwal*, *A.*, Authentication Overview, 2012

Using 2FA introduces complexity into this process, as the user now has to additionally provide something they have. In the case of SMS 2FA there are now multiple database tables needed to store passwords, phone numbers and the codes sent via SMS[10]. Additionally, software needs to be integrated which generates the codes and sends them to the user. Managing this complexity and ensuring security for all components is both time- and cost-intensive.

[9] Cp. *Basavala*, *S. R.*, *Kumar*, *N.*, *Agarrwal*, *A.*, Authentication Overview, 2012, p. 400.
[10] Cp. *Basavala*, *S. R.*, *Kumar*, *N.*, *Agarrwal*, *A.*, Authentication Overview, 2012, p. 400.

2.2 Single Sign-On and Federated Identity

2.2.1 Definitions

SSO is a mechanism which allows users to sign into multiple independent software systems using a single set of credentials[11]. It also only requires the user to perform a single action to authenticate for multiple participating services. Such systems or services could be apps, websites or technical interfaces like Application Programming Interfaces (APIs). After signing in, the user is not asked to re-enter their password when visiting a different service.[12]

SSO is made possible by an Identity Provider (IdP), which provides a central server for authentication. When talking about SSO, the website operator is usually refered to as the Service Provider (SP). Users authenticate with the IdP which shares the user's identity information with the SP.[13,14] The SP does not confirm the user's identity in any way, so they have to trust the IdP to correctly deliver user identities[15]. Originally, SSO could only be used by members of a single organization to sign into different applications like HR software, payroll or communication systems because there were no open standards that allowed companies to share identities with other organizations.[16]

Federated Identity Management (FIM) is the broader term for managing user identities across apps and websites from different organizations and companies. It provides standards which companies can use to share user identities between trusted domains, which allows SSO to be deployed not just in organizations, but also on the open web. These standards are what allows end-users to use IdPs like Google and Facebook to sign into many different websites.[17,18]

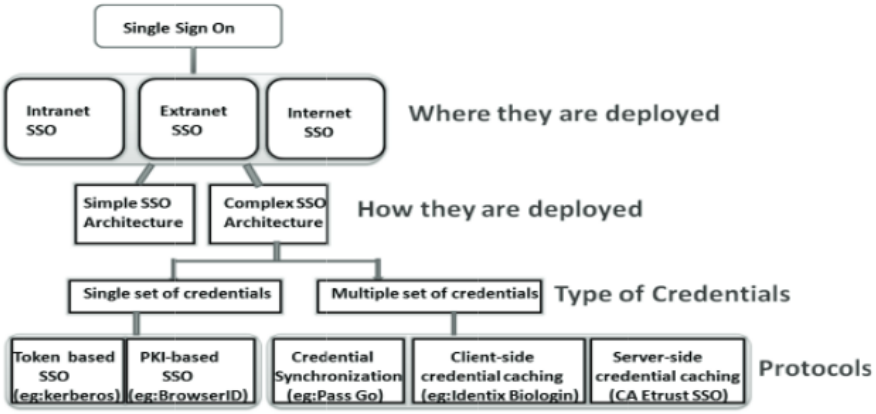
2.2.2 Types & Use Cases of SSO

Figure 2 shows the different types of SSO. Intranet SSO is used within the secure network of an organization and allows its members to access multiple applications with one set of

[11] Cp. *Radha*, *V.*, *Reddy*, *D. H.*, Survey SSO Techniques, 2012, p. 134.
[12] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 18.
[13] Cp. *Beltran*, *V.*, Characterization Web SSO, 2016, p. 24.
[14] Cp. *Bauer*, *L.* et al., User Willingness to use Social Login, 2013, p. 25.
[15] Cp. *Nallathamby*, *J.*, Federated Identity Management, 2018.
[16] Cp. *Okta*, Unterschied FIM u. SSO, n. d.
[17] Cp. ibid.
[18] Cp. *Miculan*, *M.*, *Urban*, *C.*, Analysis Facebook Connect, 2011, p. 1.

credentials. This is relatively easy to deploy, as all components and clients are administrated by the same organization, eliminating the need for open standards and trust to third parties. Extranet SSO connects SPs from different organizations. This is the basis for Web SSO and by extension Social Login, which is the type this paper is mainly concerned with. It is based on web technologies and allows users to access different public websites with a single set of credentials.[19]

Figure 2: Types of Single Sign-On



Source: *Radha*, *V.*, *Reddy*, *D. H.*, Survey SSO Techniques, 2012

2.2.3 Web SSO Protocols & Technologies

There are many different protocols defined for SSO. Some are only used for Intranet SSO, which is not covered in this paper. The next section only covers the three most used Web SSO protocols[20].

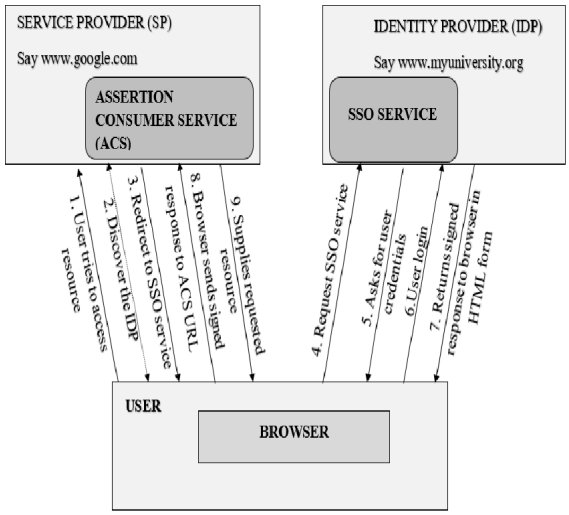
Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an open standard for exchanging user identities and authorization information between an IdP and an SP[21]. It uses the Extensible Markup Language (XML) for communication between applications. The typical authentication flow using SAML is shown in figure 3. An SP contacts an IdP and requests a user identity. The SAML standard does not specify how the IdP has to authenticate the user, but only defines the communication between the two parties. After the user has authenticated with the IdP, the identity information is sent back to the SP. It includes, whether the user is authenticated, what roles and rights they have and which data and resources they

[19] Cp. *Radha*, *V.*, *Reddy*, *D. H.*, Survey SSO Techniques, 2012, p. 135.
[20] Cp. *OneLogin*, Federated Identity Technologies, n. d.
[21] Cp. *Gross*, *T.*, SAML Security Analysis, 2003, p. 1.

are allowed to access.[22] Note that, while the SP basically communicates directly with the IdP, all communication still goes through the user's client. Which IdP is used is predefined by the SP. The user does not get to choose, where they enter their credentials or who provides their identity.[23] The SP has to trust the IdP completely, because it also handles authorization.

Figure 3: Flow of SAML Protocol



Source: *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 21

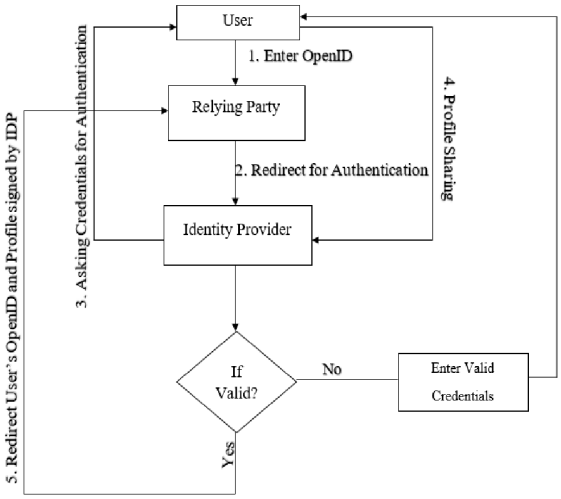
OpenID

This protocol works differently than SAML, in that the user gets to choose who provides their identity. They might use a large IdP like Google or Facebook or even set up their own OpenID service. The SP is called the Relying Party (RP) in this model. The IdP is only responsible for authentication of users and providing identity. It does not deliver any authorization information.[24] The flow is shown in figure 4.

The user visits the website and clicks the sign in button. They are then prompted to enter their OpenID IdP. The RP (the website) then redirects the user to the site of the IdP, where the user authenticates by entering their credentials. In the next step the user tells the IdP which information they want to share with the RP. If the credentials are valid, the selected identity information is passed to the RP, otherwise the user is asked to enter valid credentials.[25] This seperation of RP and IdP and introduction of user choice is the basis for Web SSO as it is used today, where websites allow users to choose their preferred identity provider. SAML does not allow for this, as the IdP is predefined by the SP.

[22] Cp. *Radha*, *V.*, *Reddy*, *D. H.*, Survey SSO Techniques, 2012, p. 137.
[23] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 21.
[24] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 21.
[25] Cp. ibid., p. 21.

Figure 4: Flow of OpenID Protocol



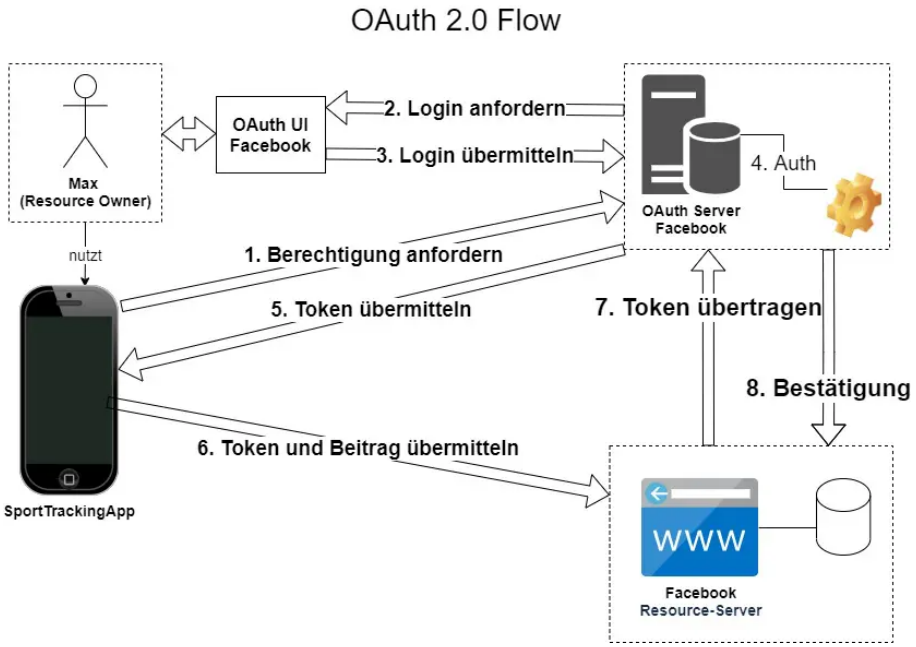
Source: *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 22

OAuth 2.0 & OpenID Connect

OAuth 2.0 differentiates from the other protocols, in that it centers around authorization rather than authentication. An example use case for this is a third-party app wanting to create a Facebook post in the user's name on their profile (see figure 5). For this, the app does not need an identity, but rather Facebook's permission to create a post. It contacts Facebook's OAuth Server and asks it for permission. Facebook then contacts the user which owns the resource (in this case the Facebook account) and asks them for permission. They accept by logging into their account and accepting access from the app. The Facebook OAuth Server sends back a token to the app which can be used to create the post. The app then contacts Facebook's resource server to actually create the post, providing the token to prove it is authorized.[26]

[26] Cp. *Wesener*, *M.*, Überblick OAuth 2.0, 2021.

Figure 5: Flow of OAuth 2.0 Protocol



Source: *Wesener*, *M.*, Überblick OAuth 2.0, 2021, p. 22

While OAuth 2.0 is a protocol specification, OpenID Connect is a concrete implementation of the protocol[27]. It also provides a way to do authentication via the OAuth 2.0 protocol, even though it was not designed for that[28]. The terms "OpenID" and "OpenID Connect" are different and can't be used interchangeably.[29]

To further understand the difference between the OAuth 2.0 and OpenID functionalities consider an e-commerce example, where the user has to enter their payment information. They have previously entered it into their Google account and would like to automatically fill the information from Google into the shop's form.

Using OpenID, the shop would use Google as an IdP to get the user's identity and automatically create a corresponding user account on the website. As OpenID simply provides the identity and can't retrieve the payment information from Google, the user would still have to enter their payment information manually. It would then be saved in the user's account on the web shop (not Google) and when they return to buy a different item, the information could be retrieved from the SP's server.

With OAuth, the SP would not have to create a user account using the identity from Google and would not have to store any information on its server. It would simply request access

[27] Cp. *Fett*, *D.*, *Kusters*, *R.*, *Schmitz*, *G.*, Security Analysis OIDC, 2017, p. 189.
[28] Cp. *Hrnjadovic*, *A.*, SSO Protocols, 2020.
[29] Cp. *Wesener*, *M.*, Überblick OAuth 2.0, 2021.

to the payment information resource from Google. The user would authenticate and allow the information transfer. Then, the SP could retrieve the information from Google and use it in the checkout process.

2.3 Web SSO Providers

2.3.1 Overview

There are many SSO solutions targeted at businesses for internal use. In addition to an IdP service they often provide an identity management suite which allows businesses to easily deploy SSO within their network.[30] The solutions targeting end users on the open web are often called "Social Login" services, as they rely on social networks that have a large userbase like Facebook, Twitter, Google or LinkedIn.[31]

The most popular social networks worldwide are Facebook with 2.9 billion and YouTube with 2.6 billion monthly active users[32]. As YouTube is based on user accounts from Google, their social login offering is examined here.

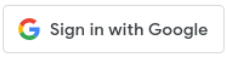
2.3.2 Sign In With Google

Google's service is based on the OAuth 2.0 protocol. This ensures a flexible service, as SPs can create a seperate account on their server, but do not have to, as they can retrieve required resources using OAuth.[33] Customizable buttons are provided by Google, which redirect the user to Google's sign in page (figure 6a). Google claims data from the feature is not used for advertising or other non-related purposes. If users are already signed into their Google account when visiting the website, Google offers the possibility to sign in with one click using a pop up, as shown in figure 6b. Google offers an additional autorization interface to allow loading other data from a users Google account.[34]

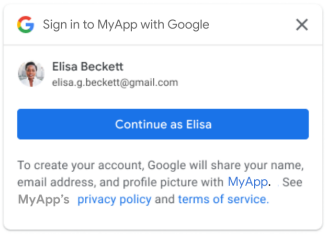
[30] Cp. *Witts*, *J.*, Top 10 Solutions for Business SSO, 2022.
[31] Cp. *Gafni*, *R.*, *Nissim*, *D.*, Factors Affecting Social Login, 2014, p. 2.
[32] Cp. *DataReportal, We Are Social, Hootsuite*, Most popular social networks, 2022.
[33] Cp. *Google*, Sign In With Google, 2022.
[34] Cp. ibid.

Figure 6: Sign In With Google UI

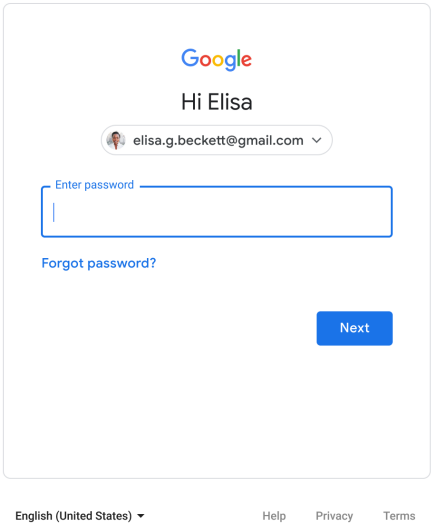
(a) Sign In With Google Button



(b) One-Tap Sign In



(c) Google Password Prompt



Source: *Google*, Sign In With Google, 2022

Integrating the Sign In With Google service into an existing website is fairly easy. SPs have to create a project on Google's developer website. They then have the option to configure the consent screen shown to the user by Google and enter information like their website name and logo, a support e-mail address and which user data the application wants to retrieve.[35]

Website developers can integrate Google's authentication interface into the website with just a few lines of code. After the user authenticates, the user data is delivered into the web application and can be used from there. If SPs have existing account management infrastructure, integrating this method might certainly require more time, as data might come in a different format or database structures might not line up.[36]

[35] Cp. *Google*, Sign In With Google, 2022.
[36] Cp. ibid.

3 Opportunities

3.1 Increasing Conversion Rates

Conversion rate is one of the most important e-commerce metrics. It gives the percentage of users who visited the website that resulted in actual sales.[37] There are a number of factors that can influence conversion rate. On the one hand these include multiple aspects that have nothing to do with the website itself. The type and range of products offered on the website are important. A store selling clothing might have a much higher conversion rate than a website selling luxury cars, for example[38]. The pricing strategy also has an impact. If the website is offering attractive pricing on their products and additional bonuses like free shipping or frequent discounts, conversion rates are increased[39]. The promotion aspect is another important factor. If the brand's advertising clearly and effectively promotes its products, visitors are more likely to buy on the first visit[40].

The factors mentioned above are related to the web presence, in that offers like discounts and free shipping need to be effectively presented on the platform. But in order to have a decent conversion rate, technical factors on the website also have to be addressed[41].

Usability is directly related to how the website is built and which features the e-commerce system has[42]. There are three dimensions of usability on a website. Information Quality describes how accurate, relevant and timely the content on the website is. Service Quality describes how interactive and responsive the website is, how good the search function works and how well the security and privacy policies are presented. System Quality includes how easy the site is to navigate, how fast the checkout process is and aspects like accessibility, and consistency of layout.[43]

Research has shown, that all three dimensions have a direct impact on conversion rates and customer retention. Users that perceive a higher information and system quality are significantly more likely to complete a purchase[44]. Service quality might have a measurable impact, but studies diverge here[45,46]. A survey shows that the second most common

[37] Cp. *Gabir*, *H. H.*, *Karrar*, *A. Z.*, Conversion Rate Website Design, 2018, p. 1.
[38] Cp. *Fatta*, *D. D.*, *Patton*, *D.*, *Viglia*, *G.*, Determinants Conversion Rates, 2018, p.165.
[39] Cp. ibid., p.165.
[40] Cp. ibid., p.165.
[41] Cp. *Gabir*, *H. H.*, *Karrar*, *A. Z.*, Conversion Rate Website Design, 2018, p. 5.
[42] Cp. ibid., p. 2f.
[43] Cp. *Kuan*, *H. H.*, *Bock*, *G.-W.*, *Vathanophas*, *V.*, Effects of Usability on Conversion and Retention rates, 2005, p. 3.
[44] Cp. ibid., p. 6.
[45] Cp. ibid., p. 6.
[46] Cp. *Gabir*, *H. H.*, *Karrar*, *A. Z.*, Conversion Rate Website Design, 2018, p. 5.

reason for adults in the United States of America (US) not completing the checkout process is, that they had to create an account. 17% said, that the checkout process was too long and complicated.[47] Additional research shows, that a requirement as simple as entering the e-mail address has a high negative impact on conversion rate[48].

Web SSO offers solutions to all factors which increase conversion rates mentioned above. By signing in with an IdP before or during the checkout process, users do not have to create a seperate account with the e-commerce site. Even for web shops that don't require users to create an account, SSO offers benefits. Traditionally users have had to re-enter their personal information like name, address, phone number and birth date with each site they were shopping on[49]. With SSO users can choose to share the information they have registered with the IdP and thus skip the process of entering their information. Thus, SSO increases the checkout speed both with required account creation and without. This also directly addresses two common reasons why customers abandon their cart during the checkout process.

Although no conclusive research could be found on this, social login might also be able to increase the number of total signups in a non e-commerce scenario. An example of this is the social media platform Reddit, which measured a 50% - 60% increase in sign ups across their desktop website and Android app after implementing Google's sign in feature[50].

3.2 Reducing Development Cost

User account management, authentication and authorization are big parts of web development and require a lot of development resources. They are also some of the most critical parts of any website, as security vulnerabilities in these areas can lead to data breaches and hacked accounts. Research is constantly being conducted in the field of password and database security and there are multiple standards, which should be adhered to in order to maximize security.[51]

The United States National Institute of Standards and Technology (NIST) publishes a set of digital identity guidelines, which outlines best practices for website developers. These include standards on implementing authentication forms, developing password criteria, storing passwords securely, designing appropriate databases and using MFA.[52]

[47] Cp. *Baymard Institute*, Cart Abandonment, 2022.
[48] Cp. *McDowell*, *W. C.*, *Wilson*, *R. C.*, *Kile*, *C. O.*, Website Design Conversion Rate, 2016, p. 4.
[49] Cp. *Beltran*, *V.*, Characterization Web SSO, 2016, p. 24.
[50] Cp. *Google*, Case Study: Reddit, 2021.
[51] Cp. *Poza*, *D.*, NIST Password Guidelines, 2021.
[52] Cp. ibid.

With SSO, the burden of implementing all these security relevant and therefore critical aspects of a website is put entirely on the IdP. Furthermore, providers like Google have an incentive to make the implementation of their SSO as simple as possible in order to boost adoption. The complexity of implementing auth and the ease of integrating SSO leads to a reduction in development resources, complexity and cost.[53]

Of course this is only the case if the website completely relies on SSO for log ins and doesn't have an additional username and password login option. In that case complexity can not be reduced, as the auth infrastructure still has to be developed.

3.3 Reducing Operation Cost

In addition to development, the administration of a website is simplified when using SSO. User data stored with the IdP does not need to be managed by the SP, reducing storage needs, operation complexity and cost. Of course, the degree of savings depends on what percentage of users is willing to adopt SSO and wether or not traditional login is still needed[54]. As shown in section 2.3.2, IdPs like Google make it possible to completely abandon account management and only use Google's identity management service. Depending on the needs of the SP, this approach might limit the functionality of the website[55].

3.4 Increasing User Security

As users signing in through social login don't have to create passwords for each website they have an account with, security is increased. On average, users seem to have between six and seven unique passwords. Each of these passwords is reused on just under six different sites, which totals an average of about 36 unique login combinations that each user has to remember.[56] Reusing the same password on multiple sites is insecure.[57] If a website is compromised and passwords are leaked to the public, hackers can try the same username and password combination on other websites to gain access. Additionally, if a user is subject to a phishing attack, hackers are able to compromise multiple of the user's accounts.[58] Even if a website is not responsible for a password leak, users hacked this way might still associate a negative experience with the brand and reduce interactions in

[53] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 22.
[54] Cp. ibid., p. 22.
[55] Cp. ibid., p. 22.
[56] Cp. *Florencio*, *D.*, *Herley*, *C.*, Password Habits, 2006, p. 4.
[57] Cp. *Pashalidis*, *A.*, *Mitchell*, *C. J.*, Taxonomy of SSO Systems, 2003, p. 249.
[58] Cp. *McDade*, *M.*, Reasons to Avoid Password Reuse, 2022.

the future. SSO eliminates this issue, as users do not need to think of new passwords for every login and are therefore not tempted to reuse the same password.

4 Risks

4.1 User Acceptance

One risk of implementing Social Login services on a website is user acceptance. According to a study in 2014, 85% of people were aware of social login features while 59.4% were already using them.[59] This number might have gone up in the mean time, as social login has become much more present across the web. A study from 2018 showed, that acceptance of social login varies within age groups and knowledge levels. Male users seem to have a higher acceptance than female users and people with knowledge about privacy related topics are more careful and use them less.[60] Additionally, some users are already used to the username and password system and might be hesitant to change their behaviours. This is supported by the password management and cloud-sync features of most modern browsers, which allow users to automatically generate and fill in passwords.[61]

Users might also not trust the social login provider to keep their personal data safe. They fear that personal information saved within their social media account is being shared with third-parties without their consent and that they thus lose their anonymity on the internet.[62,63] Users are also concerned that IdP track them on the websites they are logged in on and might be able to collect an extensive range of behaviour and user data.[64]

Lastly, being redirected to a different website and asked to log in there can be confusing for less technically literate users. As the SSO process requires this, users might get confused and shy away from these services.[65]

Because of the reasons mentioned above, if a website decides to rely solely on SSO for user logins, specific groups of users are inherently less likely to register with the website, which leads to a loss of potential customers.

4.2 Identity Provider as Single Point of Failure

Users that created an account using SSO typically do not create a seperate password with their account, as authentication is handled by the IdP. The only way for a user to sign in

[59] Cp. *Gafni*, *R.*, *Nissim*, *D.*, Factors Affecting Social Login, 2014, p. 68.
[60] Cp. *Jiang*, *J.*, Social Login Acceptance, 2018, p. 7.
[61] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 22.
[62] Cp. ibid., p. 22.
[63] Cp. *Gafni*, *R.*, *Nissim*, *D.*, Factors Affecting Social Login, 2014, p.61.
[64] Cp. ibid., p. 60.
[65] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 23.

is through the IdP.[66] This means that a given user would not be able to log in at all in the following scenarios:

- The IdP encounters an outage and their authentication service is unreachable.
- The IdP encounters data loss and is not able to provide the necessary identity information.
- The IdP terminates their service indefinitely.

While the first scenario would only result in a temporary inability to sign in, the others could result in a permanent loss of all users that signed in using that specific IdP.[67] This means that the SP is heavily dependent on the IdP to have uninterrupted availability and to never terminate their service[68]. There are ways to recover these accounts (e.g. e-mail account reset), but this only works if the SP has stored the appropriate user information on their own server, which might not always be the case.

4.3 Security of SSO Technologies

Researchers have found security flaws in many widely used SSO implementations. This includes OpenID but also specific implementations from Google and Facebook.[69] Although such vulnerabilities usually get patched very quickly[70], this might still give hackers the opportunity to attain the identity of a different user and act in their name. Most of the vulnerabilities stemmed from problems on the side of the SP, which used the given SSO protocol in a way that the IdP did not anticipate[71]. Security issues like these are very hard to recognize as they depend on the specific implementation on each website. The security benefits of not having to store passwords are thus negated by the possibility of having an insecure SSO implementation.

4.4 Security Standards of Identity Providers

The complete reliance on an IdP for authentication also has implications for security. The IdP gets to choose which security guidelines they implement, what password criteria they

[66] Cp. *Bazaz*, *T.*, *Khalique*, *A.*, SSO Review, 2016, p. 24.
[67] Cp. ibid., p. 22.
[68] Cp. *Sun*, *S.-T.* et al., A billion keys, 2010, p. 62.
[69] Cp. *Wang*, *R.*, *Chen*, *S.*, *Wang*, *X.*, Security Study of Commercial Web SSO, 2012, p. 376.
[70] Cp. ibid., p. 370-375.
[71] Cp. ibid., p. 376.

define, whether or not they require the use of MFA and how their password databases are secured. If the IdP relies on bad security practices, this directly reflects on the security of the SP. Hackers taking over a user's account with the IdP leads to them also getting access to the user's data on the SP's site.

Making this worse, SPs have a limited amount of flexibility. If a percentage of their userbase has signed in through an SSO provider, it is not possible to switch off of that provider without losing those users. This further strengthens the dependency on IdPs.

5 Conclusion

In conclusion, Web SSO and Social Login are exiting technologies that give SPs a lot of additional ways to offer quick and easy sign in functionality to their users. This paper has shown, that the technology provides operators of web platforms and e-commerce sites with many opportunities to improve their business metrics, security and usability if they are willing to manage the risks. Table 1 summarizes the opportunities and risks presented in sections 3 and 4.

Table 1: Opportunities and Risks of using SSO on websites

Opportunities	Risks
Increasing Conversion Rates	User Acceptance
Reducing Development Cost	IdP as single point of failure
Reducing Operation Cost	Security of SSO technologies
Increasing User Security	Security Standards of IdPs

It has to be mentioned, that many of the discussed opportunities like reducing development cost are only fully applicable, if SSO completely replaces traditional login with username and password. On the other hand, this greatly increases risks like dependency on the availability of IdPs.

Lastly, it is important to understand the limits of this paper. The examined aspects only cover a subset of the possible risks associated with SSO. Focus was put on the Social Login aspect of SSO targeted at businesses providing services to end users on the public web. Mainly the technical and business aspects of SSO were focused, leaving out possible risks in other areas like the legal perspective of Social Login[72]. Most of the opportunities outlined in the paper only apply to businesses that develop their own websites. The possible existence of frameworks or services that might provide simple solutions to account management were not taken into consideration. All-in-one solutions like Wix or Shopify were also not considered.

[72] Cp. *Karegar*, *F.* et al., Informed Decision about Social Login, 2018.

Bibliography

Basavala, *Sreenivasa Rao*, *Kumar*, *Narendra*, *Agarrwal*, *Alok* (Authentication Overview, 2012): Authentication: An overview, its types and integration with web and mobile applications, in: 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, s.l.: IEEE, 2012-12

Bauer, *Lujo*, *Bravo-Lillo*, *Cristian*, *Fragkaki*, *Elli*, *Melicher*, *William* (User Willingness to use Social Login, 2013): A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality, in: Proceedings of the 2013 ACM workshop on Digital identity management, s.l.: ACM, 2013-11

Bazaz, *Tayibia*, *Khalique*, *Aqeel* (SSO Review, 2016): A Review on Single Sign on Enabling Technologies and Protocols, in: International Journal of Computer Applications, 151 (2016), Nr. 11, pp. 18–25

Beltran, *Victoria* (Characterization Web SSO, 2016): Characterization of web single sign-on protocols, in: IEEE Communications Magazine, 54 (2016), Nr. 7, pp. 24–30

Fatta, *Davide Di*, *Patton*, *Dean*, *Viglia*, *Giampaolo* (Determinants Conversion Rates, 2018): The determinants of conversion rates in SME e-commerce websites, in: Journal of Retailing and Consumer Services, 41 (2018), pp. 161–168

Fett, *Daniel*, *Kusters*, *Ralf*, *Schmitz*, *Guido* (Security Analysis OIDC, 2017): The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines, in: 2017 IEEE 30th Computer Security Foundations Symposium (CSF), s.l.: IEEE, 2017-08

Florencio, *Dinei*, *Herley*, *Cormac* (Password Habits, 2006): A Large Scale Study of Web Password Habits, tech. rep. MSR-TR-2006-166, s.l., 2006-11, p. 10, URL: https://www.microsoft.com/en-us/research/publication/a-large-scale-study-of-web-password-habits/

Gabir, *Hamim Hamid*, *Karrar*, *Azza Z.* (Conversion Rate Website Design, 2018): The Effect of Website's Design Factors on Conversion Rate in E-commerce, in: 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), s.l.: IEEE, 2018-08

Gafni, *Ruti*, *Nissim*, *Dudu* (Factors Affecting Social Login, 2014): To Social Login or not Login? Exploring Factors Affecting the Decision, in: Issues in Informing Science and Information Technology, 11 (2014), pp. 057–072

Gross, *T.* (SAML Security Analysis, 2003): Security analysis of the SAML single sign-on browser/artifact profile, in: 19th Annual Computer Security Applications Conference, 2003. Proceedings. s.l.: IEEE, 2003-12-08

Jiang, *Jinglu* (Social Login Acceptance, 2018): Social Login Acceptance: A DIF Study of Differential Factors, in: s.l., 2018-05

Karegar, *Farzaneh*, *Gerber*, *Nina*, *Volkamer*, *Melanie*, *Fischer-Hübner*, *Simone* (Informed Decision about Social Login, 2018): Helping john to make informed decisions on using social login, in: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, s.l.: ACM, 2018-04

Kuan, *Huei Huang*, *Bock*, *G.-W.*, *Vathanophas*, *V.* (Effects of Usability on Conversion and Retention rates, 2005): Comparing the Effects of Usability on Customer Conversion and Retention at E-Commerce Websites, in: Proceedings of the 38th Annual Hawaii International Conference on System Sciences, s.l.: IEEE, 2005

McDowell, *William C.*, *Wilson*, *Rachel C.*, *Kile*, *Charles Owen* (Website Design Conversion Rate, 2016): An examination of retail website design and conversion rate, in: Journal of Business Research, 69 (2016), Nr. 11, pp. 4837–4842

Miculan, *Marino*, *Urban*, *Caterina* (Analysis Facebook Connect, 2011): Formal analysis of Facebook Connect Single Sign-On authentication protocol, in (2011)

Pashalidis, *Andreas*, *Mitchell*, *Chris J.* (Taxonomy of SSO Systems, 2003): A Taxonomy of Single Sign-On Systems, in: Information Security and Privacy, s.l.: Springer Berlin Heidelberg, 2003, pp. 249–264

Radha, *V.*, *Reddy*, *D. Hitha* (Survey SSO Techniques, 2012): A Survey on Single Sign-On Techniques, in: Procedia Technology, 4 (2012), 2nd International Conference on Computer, Communication, Control and Information Technology(C3IT-2012) on February 25 - 26, 2012, pp. 134–139

Sun, *San-Tsai*, *Boshmaf*, *Yazan*, *Hawkey*, *Kirstie*, *Beznosov*, *Konstantin* (A billion keys, 2010): A billion keys, but few locks, in: Proceedings of the 2010 workshop on New security paradigms - NSPW '10, s.l.: ACM Press, 2010

Wang, *Rui*, *Chen*, *Shuo*, *Wang*, *XiaoFeng* (Security Study of Commercial Web SSO, 2012): Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services, in: 2012 IEEE Symposium on Security and Privacy, s.l.: IEEE, 2012-05

Internet sources

Auth0 Inc. (AuthN vs. AuthZ, n. d.): Authentication vs. Authorization, <https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization> (no Date) [Access: 2022-08-20]

Baymard Institute (Cart Abandonment, 2022): 48 Cart Abandonment Rate Statistics 2022, <https://baymard.com/lists/cart-abandonment-rate> (2022) [Access: 2022-08-21]

DataReportal, We Are Social, Hootsuite (Most popular social networks, 2022): Most popular social networks worldwide as of January 2022, ranked by number of monthly active users (in millions), <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (2022-01-06) [Access: 2022-08-21]

Drew, *Jeremy* (2FA Mandatory, 2019): Two-factor authentication becomes mandatory for many online transactions, <https://www.lexology.com/library/detail.aspx?g=d036cdcc-2f99-4da8-837f-9b1b5a08366f> (2019-07-04) [Access: 2022-08-20]

Google (Case Study: Reddit, 2021): Case Study: Reddit, <https://developers.google.com/identity/sign-in/case-studies/reddit> (2021-12-02) [Access: 2022-08-22]

Google (Sign In With Google, 2022): Sign In With Google, <https://developers.google.com/identity/gsi/web/guides/overview> (2022-07-28) [Access: 2022-08-21]

Hrnjadovic, *Ahmet* (SSO Protocols, 2020): SAML 2.0, OpenID Connect, OAuth 2.0, Delegierte Autorisierung oder Authentisierung, <https://www.scip.ch/?labs.20200910> (2020-09-10) [Access: 2022-08-22]

McDade, *Mirren* (Reasons to Avoid Password Reuse, 2022): 5 Reasons To Avoid Password Reuse, <https://expertinsights.com/insights/5-reasons-you-should-never-reuse-passwords/> (2022-01-25) [Access: 2022-08-21]

Nallathamby, *Johann* (Federated Identity Management, 2018): What is Federated Identity Management?, <https://wso2.com/articles/2018/06/what-is-federated-identity-management/> (2018-06-18) [Access: 2022-08-21]

Okta (Unterschied FIM u. SSO, n. d.): Worin unterscheiden sich föderierte Identitätsverwaltung (FIM) und Single Sign-On (SSO)?, <https://www.okta.com/de/identity-101/federated-identity-vs-sso/> (no Date) [Access: 2022-08-20]

OneLogin (Federated Identity Technologies, n. d.): Technologies Used in Federated Identity, <https://www.onelogin.com/learn/federated-identity> (no Date) [Access: 2022-08-21]

Poza, *Diego* (NIST Password Guidelines, 2021): NIST Password Guidelines and Best Practices for 2020, <https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/> (2021-01-22) [Access: 2022-08-22]

Wesener, *Maximilian* (Überblick OAuth 2.0, 2021): OAuth 2.0 – Ein Überblick, <https://blog.doubleslash.de/oauth-2-0-ein-ueberblick/> (2021-03-10) [Access: 2022-08-21]

Witts, *Joel* (Top 10 Solutions for Business SSO, 2022): The Top 10 Single Sign-On Solutions For Business, <https://expertinsights.com/insights/top-10-single-sign-on-solutions-for-business/> (2022-08-11) [Access: 2022-08-22]

Declaration in lieu of oath

I hereby declare that I produced the submitted paper with no assistance from any other party and without the use of any unauthorized aids and, in particular, that I have marked as quotations all passages which are reproduced verbatim or near-verbatim from publications. Also, I declare that this paper has never been submitted before to any examination board in either its present form or in any other similar version. I herewith agree that this paper may be published. I herewith consent that this paper may be uploaded to the server of external contractors for the purpose of submitting it to the contractors' plagiarism detection systems. Uploading this paper for the purpose of submitting it to plagiarism detection systems is not a form of publication.

Düsseldorf, 22.8.2022

(Location, Date)

(handwritten signature)