Federated Identity Primer
## CONTENTS

Preface.............................................................................................................. vii  

**Chapter 1 Introduction to Identity ...........................................................** 1  
1.1 Introduction .......................................................................................... 1  
1.2 What Is Identity? ................................................................................. 1  
1.3 The Internet Identity Problem ......................................................... 10  
1.4 Summary ............................................................................................ 11  

**Chapter 2 What Is Federated Identity? .................................................** 13  
2.1 Introduction ....................................................................................... 13  
2.2 Authentication and Authorization .................................................... 13  
2.3 Access Control .................................................................................. 24  
2.4 Federated Service Model ................................................................. 27  
2.5 Federated Identity ............................................................................. 28  
2.6 Summary ............................................................................................ 36  

**Chapter 3 Federated Identity Technologies .........................................** 37  
3.1 Introduction ....................................................................................... 37  
3.2 OpenID ............................................................................................. 37  
3.3 OAuth .................................................................................................. 40  
3.4 Security Tokens ................................................................................ 43  
3.5 Web Service Specifications ............................................................... 50  
3.6 Windows Identity Foundation ......................................................... 52  
3.7 Claims-Based Identity ...................................................................... 54  
3.8 Summary ............................................................................................ 60  

**Chapter 4 Deployment Options...............................................................** 61  
4.1 Introduction ....................................................................................... 61  
4.2 Making a Choice ............................................................................... 61  
4.3 Active Directory Federation Services ............................................. 64  
4.4 Microsoft ACS .................................................................................. 70  
4.5 Summary ............................................................................................ 88
The concept of federated identity is nothing new. In fact, it has been around a long time. It just never really caught on, partially because its usage scenarios were limited. But, that has changed. Now with the increased usage of cloud and Internet-based applications, federated identity has started to gain a lot of traction. Instances of federated identity are popping up all over the IT landscape. Not only is it being used on the Internet, but it is also being used within enterprises and other organizations. If you haven’t come across an instance of federated identity yet, you most likely will in the very near future.

WHAT TO EXPECT FROM THIS BOOK

The purpose of this book is to provide you with a general introduction to federated identity. We will talk about federated identity and the technologies used to implement it. We will not discuss actual implementation details, but we will cover all the basics you need to know in order to get started using and implementing federated identity.

We will start in Chapter 1 by going over the concept of identity. Identity can mean a lot of things. We’ll briefly cover physical identity just to give you a little background. Then we’ll get into digital identity. We’ll go over what your digital identity can be used for and why it should be protected. Finally, in this chapter we will introduce what I call the Internet Identity Problem. We’ll talk about the problem and how federated identity can be used to solve it.

In Chapter 2, we’ll start by giving a little background info and common terminology used when talking about identity management and federated identity. We will give some background on authentication, authorization, and access control. Understanding these concepts helps lay the foundation for understanding how federated identity is established and implemented. Then, we will start talking about federated identity and why you would want to use it.
In Chapter 3, we will dive into technology. There are many different methods for implementing federated identity. But, most of these methods share common technologies and protocols. This chapter will go over some of those common technologies and protocols. Once you have a good understanding of these technologies, it will make it a little easier for you to understand the different federated identity methodologies.

In Chapter 4, we will discuss some of the deployment options. There are cloud-based deployment options and on-premise options. We’ll talk about some of the things you should consider when making your decision regarding which solution to use. We will also cover two of the more commonly used solutions: ADFS 2.0 and Access Control Services.
CHAPTER 1

Introduction to Identity

Information in this chapter:

- What Is Identity?
- The Internet Identity Problem

1.1 INTRODUCTION

Before we get into federated identity, let’s just talk for a minute about identity itself. After all, if you don’t understand identity, how can you understand federated identity? Identity may seem like a straightforward concept, but it’s actually a little more complicated than people think. What makes it so complicated is the fact that someone’s overall identity encompasses a lot more factors than you might first think. My goal in this chapter is to make sure you have a good understanding of what these factors are and how they come into play. Once you understand the overall concept of identity, then we will talk about what I call the Internet identity problem. The Internet identity problem is probably why you bought this book in the first place. You are being faced with the problem, and you are hoping that federated identity is the answer.

When breaking down the concepts, it becomes apparent that we cannot fully understand federated identity until we understand identity itself. This is why this chapter is so important. So, you need to make sure that you have a good understanding of the information in this chapter before you move onto the next one. It will make the subsequent concepts a lot easier to understand.

1.2 WHAT IS IDENTITY?

To put it succinctly, your identity is the set of characteristics that make you who you are. To understand the concept a little easier, we will break your identity up into two categories: your physical identity and your digital identity. This book focuses on what is considered digital identity. But, before we can talk about that, we’ll quickly review physical identity so we can draw analogies between physical and digital
identity concepts throughout the remainder of this text. Once we paint a clear picture of what physical identity is, its main characteristics, and how it is used, we will relate them to their digital equivalents. Although physical identity and digital identity refer to two different things, the fundamental concepts are the same. Getting a good grasp on the concept of physical identity will help you get a better grasp on the concept of digital identity much more quickly.

1.2.1 Physical Identity
When related to our daily lives, your physical identity is what identifies you as a person. It consists of many different factors and is not limited to your name and mailing address. In fact, it’s much more. It encompasses everything about you: your physical characteristics, your personality, and your day-to-day behavior.

The characteristics of your physical identity can be used to help differentiate you from others. There are no two people that share all of the same physical identity characteristics. There may be two people who are close, but they’re not exactly the same. Even in the case of identical twins, they are identical in many ways, but there are still distinguishing characteristics that can be used to tell them apart. You just have to know what characteristics to look for.

1.2.1.1 Components of Your Physical Identity
Describing your physical identity is not as simple as we may think. There’s a lot more to it than what readily comes to mind. Let’s try to break it down. For starters, there are three main components that make up your physical identity: your physical characteristics, your behavior and personality, and your personal information. In this section, we will cover each of these components in more detail.

Let’s start with some of the more notable pieces of your physical identity, your physical characteristics. Your body’s physical characteristics are the easiest pieces of your identity to identify. Your body’s physical characteristics play a huge role in identifying who you are. In fact, when someone doesn’t know a person’s name or other personal information, they will generally use physical characteristics to identify that individual. Physical characteristics include height, build, age, hair color, complexion, etc.
Physical characteristics can be a very effective way of identifying someone. Often physical characteristics are the only information about a person that you may have available to you. As an example, let’s say you witnessed a crime being committed. As a witness, you will most likely be questioned by the police. Assuming you do not personally know the individual who committed the crime, the police will ask you for a physical description of the assailant. Your description of the assailant’s physical characteristics is a big part of what the police will use to track down the suspect.

In addition to the more frequently considered physical characteristics, there are others that aren’t usually readily thought of. The way you walk, the way you talk, and the way you laugh are also parts of your physical characteristics; even though these characteristics are usually less noticed by most people. For instance, everyone has a distinctive voice. Even though the differences may not be apparent to the untrained ear, with the right equipment, it is possible to differentiate someone’s voice from anyone else’s.

One key point here is that physical characteristics are usually available to be viewed by basically anyone. Anyone who can see you or anyone that comes into close proximity with you can identify some of your physical characteristics. They don’t require any special knowledge. They don’t have to know you or request your permission to view these characteristics. They are just openly available to them. In addition, unless you live in a bubble, you can’t prevent someone from seeing these physical characteristics.

The next set of physical identity characteristics consist of your behavior and what could be considered your personality. This includes your likes and your dislikes, the way you act in different situations and the attitude you display toward events in your life. For example, take your likes and dislikes. Some people like vegetables; others like me, don’t like them. This is just one way I may be different from someone else. Then there is your reaction to certain situations. Some people sweat when they get nervous, others feel queasy. Some people don’t react at all. Each person is different.

Each person has their own preferences. They behave differently in different situations. One thing to notice here is that, like your physical characteristics, your behavior and personality are something people
can observe. They might not be able to figure everything out right away. They may have to observe you over a period of time, but it’s definitely possible to figure out a person’s behavior patterns.

This brings us to the final set of physical characteristics, your personal information. There is one very big difference between your personal information and the other physical identity characteristics we talked about. Your personal information cannot simply be observed. Usually this kind of information has to be offered by the person or someone familiar with the person. Some of these characteristics include your name, your address, and your social security number. It’s very hard to figure out someone’s name or address without conducting some sort of research, even if it’s a simple online address lookup. Because of the confidentiality of this type of information, most people will not readily know this type of information about you, nor will they be able to obtain it from observation alone.

1.2.1.2 Protecting Your Physical Identity
Whenever you meet someone for the first time or fill out some sort of application, you will start by giving your name. Your name is probably your main piece of identification. Then, depending on the circumstances or context, you may need to provide more information like your address or social security number. People are generally somewhat restrictive when disclosing their address and should be very restrictive when disclosing their social security number. Before disclosing private information such as social security number, an initial screening (of varying depth) typically occurs in order to establish trust: the requestor will generally have to identify themselves and be verified as someone who is trustworthy.

This concept is more important than you might think. If we freely offer private information without verification, we put ourselves at risk, such as identity theft and fraud. Therefore, we must protect our identity. Trust plays a big part in the identity arena. We will see that the issue of trust will come up again and again as we progress through this book.

Why is trust so important? It’s important because your identity furnishes you with access to resources available only to you. You use your identity to cash checks, get credit cards, and apply for loans. If someone else were to get a hold of your identity information, they
could do all of these things in your name, without your permission and without your knowledge. Therefore, we need to ensure that only authorized individuals have access to our identity information.

There are several techniques that can be used to establish the trust needed (trustworthiness) before you can share your identity information with others. First, you could ask a person to show some sort of identification. This could be a driver’s license, a passport, or some other sort of ID card. There is always the possibility of the driver’s license or identification card being counterfeit. But, other than that, an ID card can give you some sense of comfort that a person is who they say they are.

Another way is to establish trust by using a third party. Both you and the person that you are trying to identify would have to know and trust this third party. If you trust the third party, then you can trust identifications that they make. For example, I know Mary, and Mary knows Ben. If I trust Mary, then I can believe her when she tells me who Ben is. I don’t need to have personal knowledge of Ben beforehand (Fig. 1.1).

Sometimes there will be situations where you won’t have friends in common or know the same person but you may be separated by two or more people. In this case, you trust someone that trusts someone who knows the other person. It’s not as complicated as it sounds. It’s like “a friend of a friend” tells you who someone is. This will more than likely be the more common scenario. With the large number of people that exist in the world, it’s impossible for you to have a single friend in common with everyone (Fig. 1.2).
1.2.3 Only One Physical Identity

Because your physical identity theoretically encompasses everything about you, it’s safe to say that everyone only has one physical identity. For example, most people only have one personality. You may act differently in different situations, but you still only have one personality and the different behaviors are part of the same personality.

Depending on the situation, certain aspects of your physical identity are more relevant than others. All aspects together make up your identity, but they are not all relevant to all situations. Generally, most people will only care about a subset of someone’s physical identity characteristics. That doesn’t mean that the other characteristics aren’t important, it just means they aren’t needed to identify you to a particular person. For example, unless you work at a circus, I’m sure your employer doesn’t care whether you are afraid of clowns. But, your husband or wife would probably care. Pieces of your identity don’t just go away because someone doesn’t care about those parts. They’re still a part of you; they just may not be relevant to a particular situation.

1.2.2 Digital Identity

Now that we have talked about physical identity, it’s time for use to move into digital identity. First, I would just like to point out that
from this point on, when we talk about identity, unless specifically stated otherwise, we are referring to your digital identity. Your digital identity is what identifies you in the digital world, or what some would call the computer world. This is a relatively new concept.

Originally people just simply did whatever they wanted on a computer, and nothing was tracked. This has changed dramatically over the years. The changes themselves didn’t happen rapidly, they happened over time. But, if you look at where we’re at and compare it to where we started, there is definitely a big difference.

First web sites started tracking activities. Web sites would track information about their visitors. They would track user preferences and selections. That way the user wouldn’t have to make the same selections and set the same preferences every time they visited a site. Their settings would be saved and the web site would display however they wanted it, based on those settings. In general, this was done through the use of browser cookies. Cookies are used to store user-specific information about a particular web site. Cookies are great, but, in general, the information inside a cookie could only be accessed by the site that created it, so all information was tracked individually (on a site-by-site basis).

The next step in the evolution was for web sites to start sharing information with each other. When information is shared, your first visit to a web site can be customized just for you. A lot of sites use this shared information to create customized advertising just for you. To make this possible, information is not just collected by web sites. Instead, search engines and web browsers collect and store your information so it is readily available to the various web sites you visit.

The digital world kept evolving. Nowadays, computers aren’t the only devices used to access the Internet. You can use smartphones, tablets, and a host of other devices. Almost everything you do in the digital world is tracked, and in most cases, the information is correlated with other information and shared with almost anyone who wants it and is willing to pay for it. This information is used to build a digital profile for you. This profile forms the beginnings of a digital identity. Your full digital profile also includes more detailed information.
1.2.2.1 Components of Your Digital Identity
Similar to your physical identity, your digital identity is not just something simple like your username. It’s composed of all the information that makes you who you are in the digital world. There are many components that make up your digital identity including your user account, your digital behavior, your personal information, and even various components of your physical identity.

Usually when people think about digital identity, they think about a user account. And when they think about a user account, they only think about a username (or user ID). Your user account can contain much more information than just a username. There are some fairly obvious components like your full name and your membership status. But, there are other less common components like your location and your phone number. Looking at Fig. 1.3, you can see the multitude of attributes that can be associated with a user account.

When you use the Internet there are certain digital characteristics associated with your access. You can think of these characteristics as being analogous to the physical characteristics associated with your physical identity. Most of the characteristics are easily determined by the web site or system you are accessing. Some of these characteristics

![Fig. 1.3. User account properties.](image-url)
include your IP address, the web browser you are using to access the web site, and the operating system or device you are using.

Similar to your physical identity, your digital identity includes your behavior but in this case it is your behavior in the digital world: the sites you visit, when you last logged in, the systems you use, etc. In most cases, no two people will visit the same site at the same time, using the same device. This is why your digital behavior can be used as a differentiating factor.

In fact, paying attention to a person’s digital behavior has led to a new form of authentication called risk-based authentication. In risk-based authentication, a risk score is calculated based on whether or not the current user is performing digital actions he or she usually performs. This risk score is used to determine whether or not the user will be allowed to log in.

Your digital identity can also include certain aspects of your physical identity. For example, biometrics are sometimes used as a means of authentication. In the case of biometrics, your fingerprints, your retina, or iris can all be included as part of your digital identity. Samples of certain physical characteristics are taken and stored in a user profile. This user profile is part of your digital identity, which is verified by comparing your sample at the time of login to the sample stored in your user profile.

In the digital world, there is a lot of information about you that would be considered somewhat personal. Items like your username, e-mail address, and credit card numbers. Some of this information you may give up freely, like your e-mail address, but you may think twice before sharing your credit card number. In order for you to feel comfortable submitting your credit card information to a web site, you’d probably want to first make sure that the site can be trusted.

1.2.2.2 Protecting Your Digital Identity

Just like your physical identity needs to be protected, so does your digital identity. In the digital world, there is information you might freely share, such as your e-mail address. But there is other information you shouldn’t provide unless the recipient—in this case the system receiving the information—has been identified. Giving information to the wrong
person or system can have very profound effects on your life. Similar to the loss of your physical identity information, losing your digital identity information can put you at risk of identity theft and fraud, so it’s important that you take the necessary steps to prevent your digital identity from being leaked.

One way to validate this identity is for the system to obtain a digital certificate. If a system or web site has been identified using a digital certificate, then you might be more comfortable submitting your credit card information. We will cover digital certificates in more detail in Chapter 2 but for now, know that the digital certificate specifies the name of the web site to which it was issued. The certificate was issued by a trusted authority, therefore, you trust that the information contained within the certificate is true.

1.2.2.3 Only One Digital Identity
Just like with your physical identity, you only have one digital identity. Not all web sites that you visit will care about all of your identity information. In fact, most sites will only request a small portion of your identity information. Any information that was not requested will be discarded if it is sent to the site. For example, if a web site doesn’t use your IP address in any processing, it will not request it even though that information is readily available.

1.3 THE INTERNET IDENTITY PROBLEM
Before we can propose federated identity as a solution, we must first clarify the problem we’re trying to solve. With the coming of the “cloud era,” there has been a proliferation of web-based applications. This has been a great help for companies looking to decrease their internal IT footprint but it has brought about a problem. When applications were mostly internal, administrators could configure them to support a single set of credentials. However, most providers of Internet-based services store user credentials in different places; in most cases in their own directory store or database, which are not shared with other providers. This results in users having multiple sets of credentials. In most cases, a user will have a different set of credentials for each provider.

Having to remember all of these credentials is not only cumbersome for the user. It also causes other issues. For example, each set of
credentials has its own user and password policies, which may differ from the internal corporate policies.

There have been multiple attempts to solve this problem. Providers have come up with ways to allow single sign on. Some providers allow you to create custom keys or tokens to use for login. These tokens are created based on a set of credentials that the user already has. Problems with these methods are that they are proprietary and they must be reconfigured for each new application that is brought online, at potentially great cost. Therefore, these methods do not scale very well. Other proposed solutions have similar drawbacks.

Federated identity was built to address these authentication issues. Based on standards that can be applied to any environment, the federated identity architecture is designed to allow for scaling to support a very large number of environments. In the following chapters, we will expand on federated identity and how it can be used to solve the authentication problem.

1.4 SUMMARY

Although your physical identity and your digital identity are different, the concepts are the same. Your physical identity includes your physical characteristics, your behavior, and your personal information. Your digital identity includes your digital characteristics, your digital behavior, pieces of your physical identity, and your personal information. Both your physical and your digital identities need to be protected. You need to ensure that you are not providing your information to people, systems, or web sites that cannot be trusted.

More and more people and organizations are facing the same problems when it comes to digital identities. In a world, where more and more applications and services are being offered by different service providers, there needs to be a better way for your digital identity to follow you. This is where federated identity comes in. Your identity is stored in one place and your information can be sent to applications and services that need it.