

Identity Assurance Services For Preventing Identity Theft

Submitted to the Digital Identity Protection Workshop
2008 Conference on Security and Management

Bob Pinheiro
Robert Pinheiro Consulting LLC
bp@bobpinheiro.com

Introduction

Identity theft occurs when someone uses your personal identifying information, such as name, address, birthdate, Social Security or other government identity number, without your permission for the purpose of impersonating you to commit fraud or other crimes. An especially damaging form of identity theft occurs when someone else uses your personal information to establish new credit accounts in your name, or otherwise obtains identity-dependent services using your identity information. Examples would include the establishment of new credit card accounts, new cell phone accounts, automobile loans, mortgages, and other types of credit accounts. When identity thieves open new accounts in someone else's name, and then don't pay for the charges as expected, the result is damage to the victim's credit history, as well as bills that are eventually sent to victims for charges incurred by the identity thieves.

Medical identity theft, in which medical services are obtained using someone else's identity, is another form of this crime and results in medical expenses being charged to the identity theft victim. Medical identity theft is also dangerous because the identity theft victim's medical history is contaminated by medical diagnoses and treatments that pertain instead to the thief. Although identity theft has many forms, this paper primarily focuses on identity theft as it relates to identity claims made in conjunction with online establishment of new identity-dependent accounts or services for which there is a high risk of damage or loss when a false identity is used.

We propose that one way to fight identity theft is to better verify the identity of someone who uses personal identifying information to establish a claim of identity. More specifically, we outline a scenario in which identity assurance services provided by trusted Identity Providers can enable "strong" methods of identity authentication to be used for verifying whether someone is truly who he/she claims to be during the process of establishing new identity-dependent services. In many cases, identity authentication is based on nothing more than knowledge of some shared secret, such as a password, Social Security Number, or mother's maiden name. This is single-factor authentication based on "something you know" (SYK). But because it's easy for this type of information to be compromised, stronger forms of authentication may combine SYK with other factors such as "something you have" (SYH) or "something you are" (SYA). SYH

April 11, 2008

Identity Assurance Services For Preventing Identity Theft

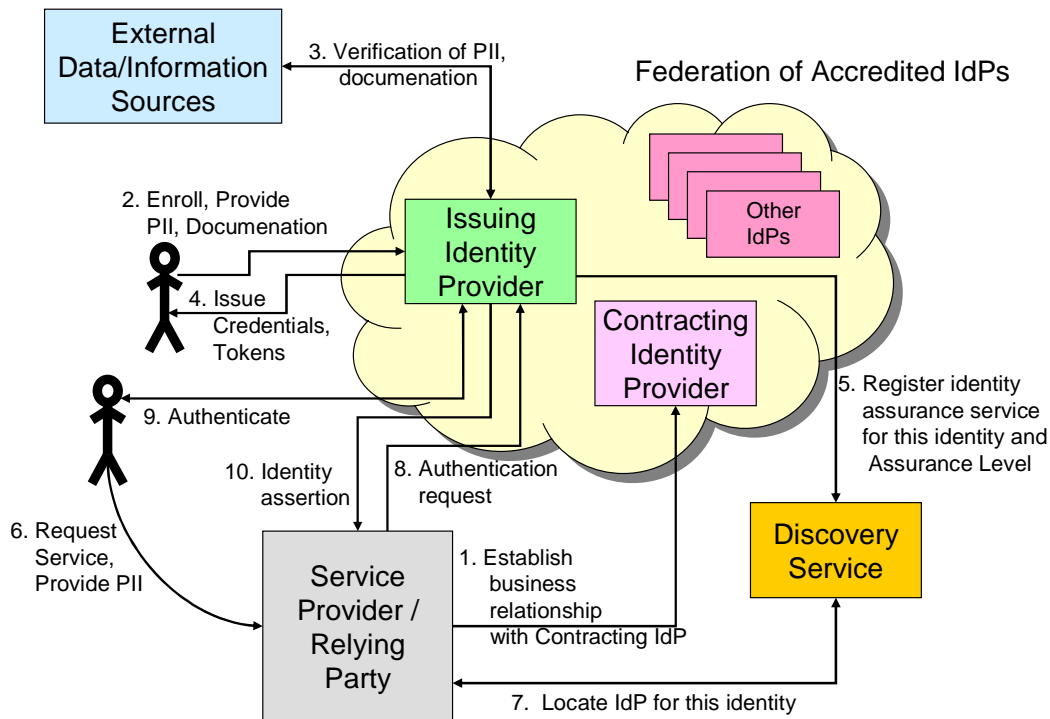
factors are generally something that must be in one's physical possession, such as a one-time password token or USB memory stick, whereas SYA factors are biometrics, such as fingerprints or voiceprints. *For our purposes, we define "strong authentication" to be multi-factor authentication that combines a SYK factor with a SYH factor and/or a SYA factor.*

The scenario described here is based upon concepts taken from the Liberty Alliance Web Services Framework, and the Liberty Alliance Identity Assurance Framework. In a nutshell, we propose that the Liberty ID-WSF and IAF provides a basis for establishing large-scale federations of trusted Identity Providers who are able to either confirm or reject an identity claim, based upon identity assurance services that enable strong authentication of identity claims using previously issued digital identity credentials associated with the claimed identity.

The use of better identity authentication as a means for preventing identity theft is one of the topics discussed within the Liberty Alliance Identity Theft Special Interest Group, a public forum for the discussion of identity theft related issues.

Strong Authentication Scenario

The basic strong authentication scenario is illustrated in the figure below.



Identity Assurance Services For Preventing Identity Theft

The actions depicted in this scenario may be described as follows:

1. A Service Provider that offers identity-dependent services decides that it wishes to be able to rely on identity assertions issued by Identity Providers that it trusts. Service Providers that rely on such identity assertions for helping to verify the identities of those who seek its services are also called Relying Parties. The Service Provider/Relying Party is assumed to trust such an assertion if the Identity Provider has been accredited as conforming to the Liberty Alliance Identity Assurance Framework, which sets forth rules and criteria for establishing trust between Relying Parties and Identity Providers. But because Identity Providers are also providing a type of service (an “identity assurance” service) to Relying Parties, the Relying Party may also need to have some type of business relationship with the Identity Provider. However, the Service Provider/Relying Party may not have a direct relationship with the specific Identity Provider that is able to authenticate a particular identity claim. We therefore make an assumption that the Service Provider/Relying Party has at least one business relationship with another accredited Identity Provider that is a member of the same federation of accredited Identity Providers. This relationship is established if the Service Provider/Relying Party “registers” with this other Identity Provider, which we call a Contracting Identity Provider. By registering with at least one Identity Provider that is a member of some federation of Identity Providers, and possibly signing a Relying Party agreement with this Contracting Identity Provider, we assume that the necessary business relationship can exist with any other member of the federation.
2. An individual interested in obtaining digital identity credentials for use in online transactions “enrolls” with an Identity Provider. The enrollment process consists of providing an adequate set of personal identifying information and supporting documentation to enable the Identity Provider to be able to verify the individual’s identity to a given degree of certainty. Depending upon the degree of certainty required, this interaction may take place online, or in-person.
 - An “identity” is defined here as some set of personal identifying information that can uniquely identify a particular individual, such as the set {Name, Address, Birthdate}.
3. The Identity Provider interacts with external sources to verify the identity information and documentation presented by the individual seeking digital credentials. This verification of identity for the purpose of issuing digital identity credentials is also known as “identity proofing.” The Liberty Alliance Identity Assurance Framework contains criteria for the establishment of requirements for identity proofing at several Assurance Levels.
 - Assurance Levels are defined within Liberty Alliance Identity Assurance Framework, and represent the degree of confidence with which an Identity Provider is able to authenticate the claimed identity. It is also related to the amount of risk associated with an authentication error. In situations where there

Identity Assurance Services For Preventing Identity Theft

would be a high risk of loss if an authentication error were to occur, Identity Providers that are able to provide identity assurance services at a high Assurance Level are needed.

4. Upon satisfactory completion of the identity proofing process, the Identity Provider issues digital identity credentials (at some Assurance Level) to be used for authentication of future claims to the individual's identity. For this reason, we will refer to this Identity Provider as the Issuing Identity Provider.
5. The Issuing Identity Provider registers, with a Discovery Service, the identity and Assurance Level associated with the newly issued digital identity credentials.
6. An individual visits the website of some Service Provider and requests an identity-dependent service such as a new credit card, home mortgage, cell phone service, car loan, etc. The individual presents Personal Identifying Information (PII) that establishes a claim to a particular identity. We will refer to this individual as the Claimant, and the identity referenced by this PII as the "claimed identity."
 - This PII consists of information such as name, birthdate, address, telephone number, driver's license number, social security number or government identification number, or other personal information sufficient to uniquely identify a particular individual.
 - The claimed identity may actually be the Claimant's true identity, or it may refer instead to someone else. Identity theft often occurs because a Service Provider/Relying Party assumes that the claimed identity is the Claimant's true identity, without further verification.
7. The Service Provider/Relying Party contacts a Discovery Service to determine whether the PII describes an identity that has been previously enrolled with some accredited Issuing Identity Provider. The precise nature of this Discovery Service will not be defined here, although we note that discovery services in general are addressed within Liberty Alliance's Web Services Framework specifications.
 - If no Issuing Identity Provider can be located at which the claimed identity has been previously enrolled, no further authentication is possible.
 - The Service Provider/Relying Party also determines whether any Issuing Identity Providers where the claimed identity has been enrolled are able to authenticate the identity claim at an Assurance Level specified by the Service Provider/Relying Party.
8. If the claimed identity was discovered to be enrolled at a particular Identity Provider, and the Identity Provider is able provide authentication at the appropriate Assurance Level, the Service Provider/Relying Party requests the Identity Provider to authenticate the Claimant.

Identity Assurance Services For Preventing Identity Theft

- It is possible that the claimed identity has been enrolled at more than one Identity Provider. In that case, the Service Provider/Relying Party must choose an Identity Provider using some criteria, here undefined.
9. If the Identity Provider accepts the request, the Claimant is requested to present the identity credentials and tokens associated with the claimed identity that have previously been issued. Essentially the Claimant is asked to present a credential that asserts the identity claim, as well as to demonstrate possession and control of one or more authentication tokens through some authentication protocol.
- A credential is defined as something that binds an identity to a token. Examples would include a UserID, as well as a digital X.509 certificate.
 - A token is something that the Claimant must possess and control in order to authenticate an identity claim. Examples include static passwords, one-time password generators, as well as private keys used to create digital signatures.
10. The Identity Provider returns the result of the authentication procedure to the Service Provider/Relying Party by means of an identity assertion, possibly based on the Security Assertion Markup Language (SAML).
- If the Claimant has been successfully authenticated by the Identity Provider, the Service Provider/Relying Party normally would accept the identity claim as valid, and establish the requested identity-dependent service using that identity. If the Claimant has not been successfully authenticated, the Service Provider/Relying Party rejects the Claimant's request for service.

Assumptions

- We assume that an individual requesting an identity-dependent service from a Service Provider is initially unknown to the Service Provider, and that the Service Provider must therefore verify the identity claim made by the individual. This claim of identity is made by presentation of Personal Identifying Information (PII) by the individual.
- Each individual is uniquely described by some set of PII. However, more than one set of identity attributes may uniquely describe an individual. The particular set of PII that is relevant to a Service Provider depends upon the needs of the Service Provider and the type of identity-dependent service that is being offered.
- An identity claim may be authenticated by a Service Provider by making an authentication request to a particular Identity Provider, which is an entity that is trusted by the Service Provider and that is assumed to have previously enrolled and verified the claimed identity. One mechanism by which these trust relationships may be established has been defined by the Liberty Alliance Identity Assurance Framework, which was created to foster the interoperability of diverse electronic authentication systems, as well as interoperability between identity federations. The

Identity Assurance Services For Preventing Identity Theft

Liberty IAF specifies business rules and other criteria for establishing trust relationships between Relying Parties and “Credential Service Providers.” [In this paper, we assume that the functionality of a Credential Service Provider has been incorporated into the Identity Provider.] These rules and criteria address initial identity “proofing” or verification, as well as the issuance and subsequent management of identity credentials and tokens.

- Identity Providers may offer authentication services to Service Providers/Relying Parties at different Assurance Levels. An Assurance Level corresponds to the degree of confidence that the Identity Provider has in the verified identity of those persons it has enrolled, as well as the robustness of the identity credentials the Identity Provider has issued for subsequent authentication.
- Identity Providers must verify or “proof” the identity of someone who seeks to enroll with the Identity Provider, and who will be issued credentials by the Identity Provider for subsequent online authentication. The Identity Provider may use some combination of physical documentation and knowledge of items of information that would be known to a particular individual, for initially establishing identity. Depending upon the Assurance Level at which identity proofing is done, this may occur in-person, or remotely via the Internet.
- There are several possible types of business entities that could act as Identity Providers. One possibility is that Identity Providers will emerge whose primary business is the enrollment and verification of individual identities, the issuance of digital identity credentials associated with those identities, and the subsequent authentication of identity claims based upon those credentials. Another possibility is that other types of businesses that already perform identity verification and authentication functions to meet their own needs may choose to leverage those functions and act as Identity Providers on behalf of their customers. These businesses may act to provide identity assurance services to Service Providers/Relying Parties, as well as Identity Theft prevention services to their own customers. Two types of such businesses are financial institutions and state motor vehicle agencies. Both of these entities must initially verifying the identities of customers, and subsequently issue credentials that can be used for identity authentication at later times. In particular, financial institutions have made great strides in strengthening their authentication procedures for online banking access, in response to the FFIEC guidance on Authentication in an Internet Banking Environment¹.

¹ The FFIEC Guidance requires banks to institute a form of authentication for online banking that provides greater security than the current system of relying on passwords only.

Conclusion

The strong authentication scenario presented here is one view of how better identity authentication might help to mitigate identity theft. It is dependent on the emergence of federations of trusted and accredited Identity Providers who will offer high assurance identity services that support strong authentication of individual identities. It also assumes that Service Providers/Relying Parties will desire to use such services to help ensure the identities of those seeking identity-dependent services. Such identity assurance services are themselves dependent on a trust framework such as the Liberty Identity Assurance Framework that allows relying parties to trust identity assertions from identity providers that have been accredited as conforming to accepted criteria for the management of identity assurance services.

Identity assurance services that might be used for prevention of new account identity theft could also be the basis for prevention of other types of identity fraud. One might envision that such services could be used to prevent credit card fraud, or fraudulent use of checking account numbers to make payments from someone else's bank account. Instead of verifying identity information pertaining to an individual, an Identity Provider might instead verify that a credit card number or checking account number is rightfully under the control of a given individual. The digital credentials and tokens issued by the Identity Provider to the individual consumer could then be invoked to authenticate claims of authorized use of those credit card numbers and checking account numbers when making online purchases or payments.