CIWG Scenarios, Use Cases, & Definitions v0.3

The Consumer Identity WG is concerned with those situations in which consumers seek high-value, identity-dependent services, or require access to high-value online resources. In both cases, “high-value” means that the consumer could potentially suffer considerable loss, or could be significantly harmed, if an imposter were able to obtain those services using the consumer’s identity, or gain access to those online resources belonging to the consumer.

Definitions of terms used can be found following these Scenarios and Use Cases.

Scenario A

An Identity Provider issues an identity assertion/claim for verification of identity after multifactor authentication of the consumer at Assurance Levels 3 or 4 as defined by NIST 800-63, Kantara Identity Assurance Framework, or the equivalent

Examples:

- Consumer wants to open a new credit card at an online banking site
- Consumer wants to open a new charge card at an online merchant
- Consumer wants to apply for a loan at an online banking site
- Consumer wants to access his/her free credit report from annualcreditreport.com, or obtain his/her credit score from a consumer credit reporting agency
- Consumer wants to change his/her social security beneficiary information, or mailing address, at the Social Security website
- Consumer's Personally Identifiable Information (PII) has been stolen and may be used by an imposter to claim the consumer's identity for establishment of a new high value relationship with a Service Provider

Use Case 1

Service Provider initiates request for a SAML identity assertion from a trusted Identity Provider

Consumer has had his/her identity verified by a trusted Identity Provider, and has been issued a credential and token for use online.

1. Consumer presents credential to the Service Provider.
2. Service Provider determines whether there exists an Identity Provider that it trusts that can authenticate the credential.
3. If a trusted Identity Provider can be located, Service Provider redirects the consumer to the Identity Provider, or activates a pop-up window to the Identity Provider.
4. Consumer presents the credential to the Identity Provider (or credential is presented to the Identity Provider in the redirection process).
5. Using an authentication protocol, Identity Provider determines whether the consumer possesses and controls an authentication token that corresponds to the presented credential. If so, the credential has been successfully authenticated.
6. If the credential is successfully authenticated by means of the token, Identity Provider assumes that the person presenting the credential is the same person whose identity was initially verified by the Identity Provider, and to whom it issued the credential. Identity Provider returns a secure SAML (or equivalent) identity assertion to the Service Provider / Relying Party containing a set of verified identifier values pertaining to the consumer. If the credential is not successfully authenticated, Identity Provider returns that information to Service Provider in the same manner.

Use Case 2

Service Provider initiates request for a verified identity claim by invoking a selector / active client and a managed Information Card

Consumer has had his/her identity verified by an Identity Provider, and has been issued a managed Information Card and token for use online.

1. Consumer requests an identity-dependent service from a Service Provider.
2. Service Provider returns its identity policy to the consumer’s computer, stating the identifiers that must be verified in order to obtain the service.
3. If the consumer has a managed Information Card residing in the consumer’s selector/active client that corresponds to those identifiers, and which was issued by an Identity Provider trusted by the Service Provider, then the selector/active client displays the card on the consumer’s screen, and the consumer selects the card.
4. Consumer authenticates to the Identity Provider using the appropriate token.
5. If authentication is successful, Identity Provider returns (via consumer) a verified and cryptographically-signed identity assertion (called a Claim) to the Service Provider / Relying Party containing the necessary identifier values pertaining to the consumer.

Use Case 3

Service Provider requests Personally Identifiable Information (PII) from the consumer to establish identity

The Service Provider has access to a credit bureau or other data service that is used to verify the credit staus of the consumer, or to verify an identity claim on the basis of knowledge-based authentication. The Service Provider collects PII from someone seeking to establish a new relationship, and submits it to the credit bureau / data service, where it is matched against a record on file with the credit bureau / data service. There are two alternative subcases:

Subcase 3a

Credit bureau or data service is unaware of any digital identity credentials associated with the person whose PII was submitted

This subcase is equivalent to the current mode of operation. A credit bureau reports on the credit status of the person whose PII it matched. A data service prompts for knowledge-based questions to verify identity. There is no use of digital identity credentials for further verification of identity.

Subcase 3b

Credit bureau or data service is aware that a digital identity credential has been issued by some Identity Provider to the person whose PII it matched, and is willling to act as an intermediary to facilitate identity authentication

1. Consumer presents his/her PII to the Service Provider in order to establish an identity claim for the purpose of obtaining a new identity-dependent service.
2. Service Provider provides PII to the credit bureau or data service.
3. Credit bureau or data service matches PII to one of its records, which corresponds to a particular consumer, and identifies an Identity Provider that can authenticate the identity claim, if one exists.
4. In a yet to be defined way, the credit bureau or data service facilitates an interaction between the Identity Provider, the person who presented the PII and is claiming an identity, and the Service Provider. The outcome of this interaction is a notification to the Service Provider that allows the Service Provider to determine, with a high degree of confidence, whether this person is who he/she claims to be. Note: It is possible that the credit bureau or data service could be the Identity Provider.

Scenario B

An Identity Provider issues an identity assertion/claim for verification of one or more personal attributes after authentication of the consumer at an appropriate Assurance Level as defined byNIST 800-63, Kantara Identity Assurance Framework, or the equivalent

A consumer wishes to obtain a service from a Service Provider that is dependent on one or more personal attributes (e.g., age, membership in some organization, etc.), but does not want to divulge his/her identity to the Service Provider.

Use Case 1

Service Provider initiates request for a SAML identity assertion from a trusted Identity Provider

Consumer has had his/her personal attributes verified by an Identity Provider, and has been issued a credential and token for use online.

1. Consumer requests an attribute-dependent service from a Service Provider, and presents a credential to the Service Provider.
2. Service Provider determines whether there exists an Identity Provider that it trusts that can authenticate the credential.
3. If a trusted Identity Provider can be located, Service Provider redirects the consumer to the Identity Provider, or activates a pop-up window to the Identity Provider.
4. Consumer presents the credential to the Identity Provider (or credential is presented to the Identity Provider in the redirection process).
5. Using an authentication protocol, Identity Provider determines whether the consumer possesses and controls an authentication token that corresponds to the presented credential. If so, the credential has been successfully authenticated.
6. If the credential is successfully authenticated by means of the token, Identity Provider assumes that the person presenting the credential is the same person whose personal attributes were initially verified by the Identity Provider, and to whom it issued the credential. Identity Provider returns a secure SAML (or equivalent) identity assertion to the Service Provider / Relying Party containing a set of relevant attribute values pertaining to the consumer. If the credential is not successfully authenticated, Identity Provider returns that information to Service Provider in the same manner.

Use Case 2

Service Provider initiates request for a verified identity claim by invoking a selector / active client and a managed Information Card

Consumer has had his/her personal attributes verified by an Identity Provider, and has been issued a managed Information Card and token for use online.

1. Consumer requests an attribute-dependent service from a Service Provider.
2. Service Provider returns its identity policy to the consumer's computer, stating the personal attributes that must be verified in order to obtain the service.
3. If the consumer has a managed Information Card residing in the consumer's selector/active client that corresponds to those attributes, and which was issued by an Identity Provider trusted by the Service Provider, then the selector/active client displays the card on the consumer's screen, and the consumer selects the card.
4. Consumer authenticates to the Identity Provider using the appropriate token.
5. If authentication is successful, Identity Provider returns (via consumer) a verified and cryptographically-signed identity assertion (called a Claim) to the Service Provider / Relying Party containing the necessary attribute values pertaining to the consumer.

Scenario C

Consumer access to existing high-value online resources, records, or accounts using strong authentication

A consumer needs to access, on a repeated basis, some high-value, online resource that the consumer has previously enrolled in, such as an online financial account, online payment account, online medical records, etc. Access to these resources requires "strong" authentication; i.e. usually multifactor authentication requiring a password together with some other type of token.

Use Case 1

Personal X.509 certificate

1. Service Provider initially binds the consumer's certificate (containing the consumer's public key) to the online resource/account.
2. Returning consumer presents the certificate to identify the resource/account he/she is seeking access to.
3. Consumer uses the corresponding private key as a token to authenticate a claim of authorization to access the online resource/account, according to a well-defined challenge/response authentication protocol.

Use Case 2

OpenID using strong authentication

1. Service Provider initially binds an OpenID URL or email address, or an OpenID represented in a selector/active client, to the online resource /account.
2. When attempting to access the protected resource, the returning consumer presents the OpenID, and is redirected to the appropriate OpenID Identity Provider (OP).
3. Authentication occurs via a strong authentication method, such as a challenge/response protocol involving the consumer's digital certificate and private key, or by presentation of a one-time password. (Authentication by static password is deemed to be "low assurance" authentication, and not permitted).
4. An identity assertion is sent from OP to Service Provider / Relying Party containing the authentication result.

Use Case 3

Self-issued Information Card based on X.509 certificate

1. Service Provider initially binds the consumer's self-issued Information Card to the online resource/account.
2. When attempting to access the protected resource, the Service Provider sends a message to the consumer's computer, causing the consumer's selector/active client to display the appropriate self-issued Information Card.
3. Consumer selects the Information Card and "unlocks" the card using a PIN or password.
4. A cryptographically-signed electronic message is returned to the Service Provider / Relying Party, affirming (or negating) that the authorized self-issued Information Card has been presented.

Definitions

- A Service Provider is any provider of an identity-dependent online service. Examples of Service Providers include blogging services, Twitter, financial institutions, medical establishments, websites that provide credit reports and credit scores to consumers, online payment services, etc.
- An Identity is some set of identifiers (e.g., name, address, social security number, birthdate, nationality, etc.) about a person seeking an identity-dependent service that the Service Provider needs to know. These identifiers are a subset of the Personally Identifiable Information (PII) that can be associated with a consumer.
- A Credential is something that is presented by a consumer to a Service Provider in order to claim an identity. Examples include username or loginID, URL or email address, X.509 certificate, PII, driver's license or passport (in the physical world).

- A Token is something that a consumer uses to authenticate the identity claim made by the Credential, by demonstrating possession and control of the token according to a well-defined authentication protocol. Examples include static password, PIN, X.509 private key, one-time password, biometric.

- An Identity Provider is an entity that:
    - Has verified the identity (or other personal attributes) of an individual consumer to a certain degree of assurance
    - Has issued to the consumer a credential (or managed Information Card) and token
    - Can issue an identity assertion/verified claim at a certain assurance level, containing an appropriate set of identifier or attribute values pertaining to the consumer, as a result of authentication of the consumer's credential as specified by the authentication protocol.

- An Information Card is a kind of electronic identity card; it represents a certain set of identifiers or attributes (called metadata) but does not contain specific values for those things. Managed Information Cards are issued by an Identity Provider. Self-issued Information Cards are created by the consumer.

- OpenID is an open, decentralized standard for authenticating users to websites.

- A Selector or Active Client is a kind of electronic wallet that holds and displays Information Cards that can represent identity claims or OpenIDs.

- Assurance refers to the degree of certainty surrounding a claim of identity. One such measure of assurance is specified by the Kantara Identity Assurance Framework and NIST Special Publication 800-83, *Electronic Authentication Guideline*. We define "high assurance" as corresponding to Assurance Levels 3 and 4 as defined by these sources.

- A Relying Party is a Service Provider that relies on an authenticated Credential to establish the identity of a consumer who is seeking a service, or is seeking access to some resource.

- A Relying Party decides to "trust" identity assertions/claims from a particular Identity Provider in several ways, including previously established bilateral agreements as well as determining that the Identity Provider conforms to a set of criteria specified by a formal identity assurance framework.

- An Identity Assurance Framework is a set of baseline policy requirements (criteria) and rules against which Service Providers / Relying Parties and Identity Providers establish uniform, interoperable, and trusted interactions with each other. These interactions take the form of identity assertions about some consumer issued to a Service Provider / Relying Party by an Identity Provider trusted by the Service Provider / Relying Party.

- SAML, the Security Assertion Markup Language, provides for secure transmission of identity information across boundaries; i.e., it allows an Identity Provider to securely transmit an identity assertion to a Service Provider / Relying Party.