Consumer Identity Workgroup
Interim Report
October, 2010

Date: 2010-10-14

Editor: Bob Pinheiro

Contributors: Bob Pinheiro, Jeff Stollman, Sal Khan

Status: This document is a **Kantara Initiative Work Group Report**, approved by the Consumer Identity WG (see section 3.9 and 4 of the Kantara Initiative Operating Procedures)

Abstract:
This Interim Report consists of a Executive Summary, followed by a series of slide images that describe the high assurance consumer identity problem that CIWG is trying to address, as well as questions that need to be answered in seeking to provide solutions. It also describes CIWG's deliverables and next steps.

Following this are three appendices that capture material already present on the CIWG website. This material established the basis for defining the high assurance consumer identity problem that CIWG seeks to address.

- **Appendix A** describes high assurance consumer identity "needs", and the corresponding needs of Service Providers / Relying Parties to satisfy consumer needs.
- **Appendix B** contains scenarios and uses cases previously proposed that describe an abstract view of the identity assertions or claims pertinent to high assurance consumer transactions.
- **Appendix C** contains definitions of terms used throughout.

Filename: CIWG-Interim-Report-Oct-2010

Notice:

Executive Summary

Online services for consumers that involve "high value" financial transactions or payments, including the establishment of new high value relationships and accounts, are prime targets for various types of identity fraud. With the advent of electronic patient records and personal data stores, the opportunities for harm to consumers as a result of fraudulent access to sensitive information becomes even greater. While consumers may not necessarily articulate a "need" to carry around hard tokens or other forms of high assurance identity credentials to deal with these problems, they would almost certainly state a need to prevent others from "stealing their identities" by breaking into their bank accounts, obtaining new credit cards in their name, accessing their sensitive personal and medical information, or otherwise impersonating them in situations where the outcome can be harmful to the consumer. These needs can only be met when strong authentication methods and "open identity" technologies can be combined to create high assurance consumer identity solutions in a way that is easy for consumers to use and understand, and that protects consumer's privacy as well. One aspect of the privacy issue is that high assurance identity-related claims should only be necessary in high value transactions.

Although the focus of CIWG is consumer identity, it is not only consumers that benefit if identity theft can be prevented. To the extent that consumers can avoid these kinds of identity fraud, service providers also benefit as a result of reduced financial loss, as well as limiting potential liability and damage to their reputations.

Strong authentication technologies already exist, of course, but have not seen widespread deployment and use in consumer applications. This is due to factors including usability, convenience, education and awareness, cost, and weak motivation for better fraud prevention. However, as criminals find new ways to steal personal information and use it to enable identity-related crimes against consumers, it's clear that identity fraud prevention requires more than attempting to keep personal information secure. What's needed are better ways for service providers to authenticate identity-related claims, as well as stronger motivations for their use in high value transactions.

This Interim Report describes the identity theft/fraud problem, and advocates that the solution is to enable (and motivate) service providers to rely on high assurance, identity-related claims during the establishment of new high value services or relationships, and as a condition for granting access to previously-established high value services or protected resources. This Interim Report also enumerates various issues that need to be addressed in order to do this. Such issues include:

- Will different "trust communities" such as financial services, healthcare, etc., seek to define their own trust frameworks, with differing criteria for what constitutes a high assurance assertion, identity proofing, or acceptable authentication technologies for high assurance claims?

- Will consumers be able to use the same credentials or authentication tokens for authentication to service providers / relying parties in different trust communities?

- Will consumers be able to access all their credentials and/or authentication tokens from the same digital "wallet" or active client?

- How will consumers obtain and deploy the necessary credentials / tokens / active clients?

- How should the definition of "high assurance" change to account for consumer-related claims other than claims of identity; for instance, claims of authority to access protected online resources, or claims of authority to make an online payment from a payment account, or to move money out of an online financial account?

- Can high assurance credentials and tokens issued to consumers for authentication of identity claims by an identity provider also be used for non-assertion based authentication of consumers to service providers / relying parties for frequent, ongoing access to protected resources; that is, without relying on assertions from an identity provider?

The ultimate goal of the Consumer Identity WG is to provide specific recommendations to help ensure that emerging identity infrastructures can enable high assurance claims of identity or authorization needed to prevent identity theft and other types of identity-related fraud affecting consumers and service providers. CIWG also seeks to understand the feasibility issues pertaining to large-scale deployments of these capabilities. In order to better approach this goal, CIWG seeks to initially create a report that describes the current state of high assurance / strong authentication applications for consumers, and that expands on the challenges and roadblocks that need to be overcome.

The ability of CIWG to produce these results is highly dependent on whether funding is available to retain necessary personnel and resources, as well as the interest and availability of volunteer WG participants.

Consumer Identity WG Interim Report

October, 2010

Chair: Bob Pinheiro
consumerid@bobpinheiro.com

kantara INITIATIVE

Consumer Identity WG

Purpose

To help ensure that emerging identity infrastructures can eliminate or reduce identity theft/fraud by supporting the needs of

- **consumers** to prevent others from fraudulently impersonating them when conducting high value online transactions,
- **service providers** to ensure they have high assurance of
  - the identity of someone who seeks to establish a high value relationship or service
  - the authorization status of someone who seeks to access (or control access to) high value, protected resources
  - the authorization status of someone who seeks to make a payment using a payment or credit card account, or to move money out of a financial account

Identity Theft Harms Consumers

Consumers are harmed if others can impersonate them for various purposes (financial, medical, etc) when sensitive personal information is stolen or misused to

- establish **high value, identity-dependent services** such as credit cards, loans, cell phone accounts, etc.
- obtain **unauthorized access to high value online resources** such as financial accounts, medical records, credit reports, etc

Consumers are Harmed by Identity Theft When…..

- Charges are incurred to them for purchases they didn't make
- Money is removed from their bank accounts by "account hijackers"
- Their credit ratings are damaged
- They suffer reputational losses
- They lose extensive time trying to remedy the situation
- Their medical records are "contaminated" by medical services provided to imposters
- They are falsely arrested when a criminal uses their identity

Identity Fraud Harms Service Providers

- Service providers are harmed and suffer losses if they provide high value services to those who fraudulently claim a false identity or authority to access a protected resource.
- Example harms to service providers include:
  - Financial losses
  - Reputational losses
  - Possible legal liability

High Value Consumer Services

Definition

- A high value service or resource is one for which the harm to a consumer may be "substantial" if an imposter is able to fraudulently establish a new relationship with the service provider, using the consumer's identity, or is otherwise able to fraudulently use such a service, or obtain unauthorized access to protected resources owned by the consumer.
  - Substantial harm is assumed to be harm that is defined as "moderate" or "high" within any of 5 categories specified by OMB Memorandum 0404, "E-Authentication Guidance for Federal Agencies".

High Value Consumer Services

Definition of Substantial Consumer Harm

OMB 0404 defines the following 5 categories of harms that are relevant to consumers:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

High Value Consumer Services

Some Examples

- Financial Services
  - New account opening
  - Access to existing online accounts
  - Transaction authorizations; ie, move money out of accts
  - Payments; e.g., credit card, debit, commercial payment services
- Healthcare
  - Access to patient health records or other patient-specfic healthcare portals
  - Impersonation of someone else to obtain medical services (Medical ID Theft)
- Government Interactions
  - Payment and reporting of taxes
  - Issuance of driver's licenses and other motor vehicle issues
- Credit Bureaus
  - Access to free online credit report
- Personal Data Stores
  - Access to personal data stores containing sensitive information
  - Authorized permissions for data access

Can Better Secured Personal Information Help Prevent ID Theft?

Maybe, BUT

- Service Providers offering high value services should not accept self-asserted personal information as "proof" of anything.
- **Service Providers need high assurance of various kinds of consumer claims.**
  - High assurance ➔ FRAUD PREVENTION
  - Otherwise, just use low assurance, self-asserted identity or other claims
- Consumers need high assurance that false claims made by others using their personal information to obtain high value services will be rejected.

What is "High Assurance"?

- OMB 0404 defines 'high assurance" as pertaining to the confidence a service provider has in an asserted identity's validity.
- Tightly coupling "high assurance" with "identity" may be too narrow.
- Need to re-evaluate the definition of "high assurance" to include high confidence in other types of consumer claims.

High Assurance of What??

- **Service providers** offering high value services need high assurance of various types of consumer-related claims:
  - Claim of identity
  - Claim of authority to access a protected resource
  - Claim of authority to make a payment using a payment account, or move funds from a bank account
- **Consumers** need high assurance that others cannot fraudulently impersonate them to establish or access high value services using their identities.

What's Needed to Enable High Assurance of Consumer Claims?

- NIST SP 800-63 "Electronic Authentication Guideline" specifies four assurance levels in terms of: strength of authentication technology and protocol, rigor of "identity proofing", and criteria for credential and token issuance and management.
- **High assurance of consumer claims** should therefore be the result of using strong authentication technology and protocols in combination with rigorous claims verification and corresponding criteria for issuance and management of credentials and tokens.

Where Are We Today?

- If stronger authentication can help enable high assurance identity claims and can help prevent identity fraud, why isn't everyone using it today?
- Some reasons:
  - Weak motivation; fraud is part of cost of doing business
  - Too expensive to deploy and manage on a mass scale
  - Usability and convenience issues for consumers
  - Man in the Browser: Need to authenticate transactions
  - "Token necklace" problem
- Need an "identity infrastructure" that can make strong authentication and high assurance consumer claims feasible for widespread use.

National Strategy for Trusted Identities in Cyberspace

- US federal government's NSTIC initiative seeks to facilitate the creation of an identity "ecosystem" that can help to "*raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions.*"
- CIWG seeks to help ensure that such an infrastructure can enable high assurance identity or other claims by consumers in high value transactions, in a way that
  - protects consumer privacy,
  - discourages demand for high assurance identity claims for low value services or transactions,
  - enables consumers to prevent someone else from fraudulently impersonating them in high value transactions.

Consumer Identity WG

Goals

- Investigate open issues and provide specific recommendations to help ensure that an identity infrastructure enables
  - **Service Providers / Relying Parties** to authenticate, with high assurance, relevant claims about consumers to whom they provide high value services, while protecting the consumer's privacy
  - **Consumers** to easily provide the minimal set of verified claims needed by SPs/RPs to enroll in, and use, high value services
  - **Consumers** to prevent others from fraudulently impersonating them online in high value transactions
- Determine feasibility and understand what must happen in order to "roll out" this identity infrastructure and achieve widespread adoption by consumers.

Feasibility Depends On

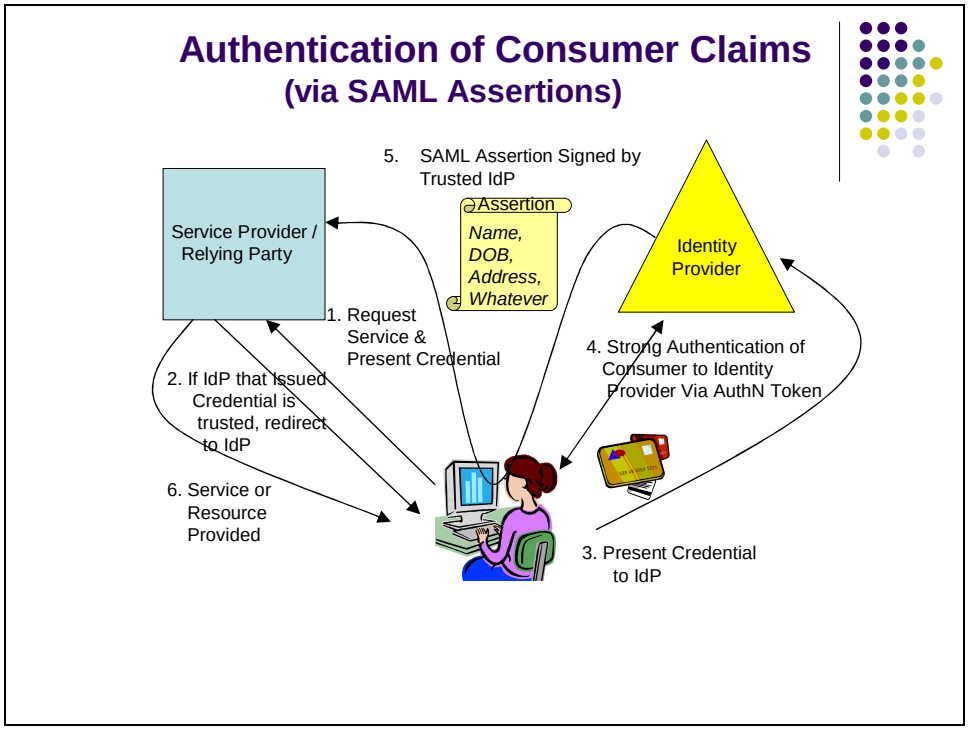
- Whether **Service Providers / Relying Parties** will place a premium on minimizing fraud in connection with high value services by demanding relevant high assurance consumer claims.
- Whether **Consumers** will perceive digital credentials and authentication methods needed for authentication of high assurance consumer claims as being easy to use.
- Whether **Identity Providers** that provide high assurance consumer claims can develop a business justification for doing so.
- Whether consumer **Privacy** can be protected
- Whether **Liability Issues** can be adequately addressed.

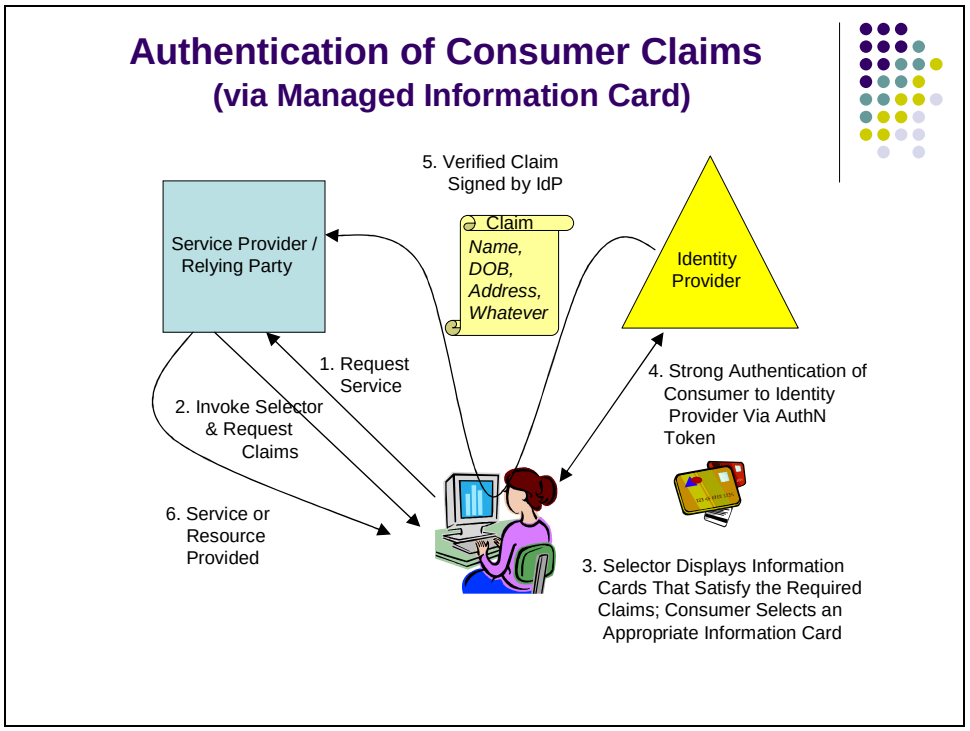
Key Identity Infrastructure Components

- **Claims** consisting of various attributes pertaining to a consumer.
- **Attributes** such as name, birthdate, or any other facts about a consumer.
- **Service Providers / Relying Parties** that provide high value online services, and that rely on claims or assertions of identity, authorization, or other claims in order to provide those services.
- **Consumers** that seek services from Service Providers.
- **Credentials and authentication tokens** that are used by consumers to make an identity-related claim, and to authenticate that claim.

Key Identity Infrastructure Components

- **Identity Providers** that issue high assurance credentials, authentication tokens, and verified claims.
- **Trust frameworks** that enable trusted transactions between Identity Providers and Service Providers/Relying Parties relying on verified assertions/claims issued by Identity Providers.
- **Selectors** or **Active Clients** that act as digital wallets and display credentials such as OpenIDs and Information Cards in the form of virtual “cards” that can be accessed by consumers for use at Service Provider / Relying Party sites.


Authentication of Consumer Claims
(via SAML Assertions)
5. SAML Assertion Signed by Trusted IdP
Assertion
Name, DOB, Address, Whatever
Service Provider / Relying Party
Identity Provider
1. Request Service & Present Credential
2. If IdP that Issued Credential is trusted, redirect to IdP
4. Strong Authentication of Consumer to Identity Provider Via AuthN Token
6. Service or Resource Provided
3. Present Credential to IdP


Authentication of Consumer Claims
(via Managed Information Card)
5. Verified Claim Signed by IdP
Claim
Name, DOB, Address, Whatever
Service Provider / Relying Party
Identity Provider
1. Request Service
2. Invoke Selector & Request Claims
4. Strong Authentication of Consumer to Identity Provider Via AuthN Token
6. Service or Resource Provided
3. Selector Displays Information Cards That Satisfy the Required Claims; Consumer Selects an Appropriate Information Card

Open Issues in High Assurance Consumer Identity

Definition of "High Assurance"

- Current trust frameworks associate "high assurance" with knowledge of an individual's identity; *identity proofing*
- Need to redefine high assurance in terms of strong authentication coupled with rigorous verification of claims by an IdP.
- "High assurance" should also pertain to claims other than identity; ie, authorization to access a resource or make a payment, claims based on other attributes such as age, membership, etc.

High Assurance of……

a consumer's identity

- Needed by Service Provider to prevent fraud when establishing new high value relationships or enrolling in high value accounts
- Requires identity assertion/verified claim from Identity Provider to Service Provider / Relying Party upon Consumer authentication to IdP

High Assurance of…….
authority to access a protected resource

- Needed by Service Provider to prevent fraudulent access to an online account or resource
- Requires EITHER:
  - Assertion/claim from an IdP verifying authZ status
  - Strong credential / authN token bound to the online resource; e.g.,
    - PKI cert/private key
    - Information Card

High Assurance of…….
authority to make an online payment

- Needed by online merchants to prevent fraudulent charges to a payment account that can result in a chargeback to merchant. For instance,
  - Credit card / debit card
  - Virtual “one time” credit card
  - Other payment services; e.g., Paypal
- Requires either:
  - Assertion/claim from a cc issuer to merchant verifying authZ status after consumer authenticates to cc issuer
  - Assertion/claim from cc issuer to merchant containing virtual cc information
  - Strong authN token bound to payment account

Open Issues in High Assurance Consumer Identity
Trust Frameworks and Claims

- Will different trust communities require different trust frameworks for supporting high value services offered by service providers in those communities?
  - Open Identity Exchange (OIX) is defining trust frameworks for different "trust communities" such as OCLC library, telecom, personal data stores, PBS public media
  - What about communities such as financial, healthcare, government, where high assurance is also important?
  - How will these trust frameworks be the same/different?
- Will different sets of claims be required by Service Providers operating in different trust communities?

Open Issues in High Assurance Consumer Identity
Credentials & Tokens

- Distinguish "credentials" from "authentication tokens"
  - A credential presents a claim made by a consumer; e.g., personally identifiable information, a userID, X.509 certificate, managed or self-issued Information Card, OpenID
  - An authentication token authenticates a credential; e.g., a password, shared secret, one-time password, X.509 private key, biometric
- Will separate credentials be needed by consumers for use within different trust communities?
- Who will provide high assurance credentials and tokens to consumers?
  - A consortium within each trust community?
  - Individual Identity Providers within each trust community?
  - State Motor Vehicle Bureaus?
  - Commercial Identity Providers; ie, Yahoo, Paypal, etc?

Open Issues in High Assurance Consumer Identity
Digital Wallets / Selectors / Active Clients

- Should selectors / active clients be the default mode of deployment for high assurance online consumer credentials?
- Will consumers be able to keep and manage their various credentials using a single selector / active client?
- What are the issues and tradeoffs determining whether selectors / active clients should be deployed:
  - on the consumer's PC or laptop or cell phone
  - "in the cloud"
  - on a portable physical device; ie, USB dongle
- Who will provide and setup these selectors / active clients on behalf of consumers?
  - Browser makers (as plug-ins)?
  - Identity Providers?
  - Consumers themselves?

Open Issues in High Assurance Consumer Identity
Digital Wallets / Selectors / Active Clients

- What is the trust relationship between cloud-based selectors and Identity Providers?
  - Does the consumer use an authN token to authenticate to the selector for access to a credential, followed by an authentication assertion from the selector to the IdP for issuance of a verified claim,
    => IdP trusts Selector
  - Does the consumer authenticate separately to the selector and to the IdP
    => No trust relationship
- Trust relationship between cloud-based selector and Relying Party?

Open Issues in High Assurance Consumer Identity
Portability of Authentication Tokens

- For credentials residing in cloud-based selectors / active clients, or on a consumer-owned device, where will the authentication tokens needed to authenticate to Identity Providers reside in order to maintain portability?
  - Also on the mobile device?
  - USB dongle?
  - Somewhere else?

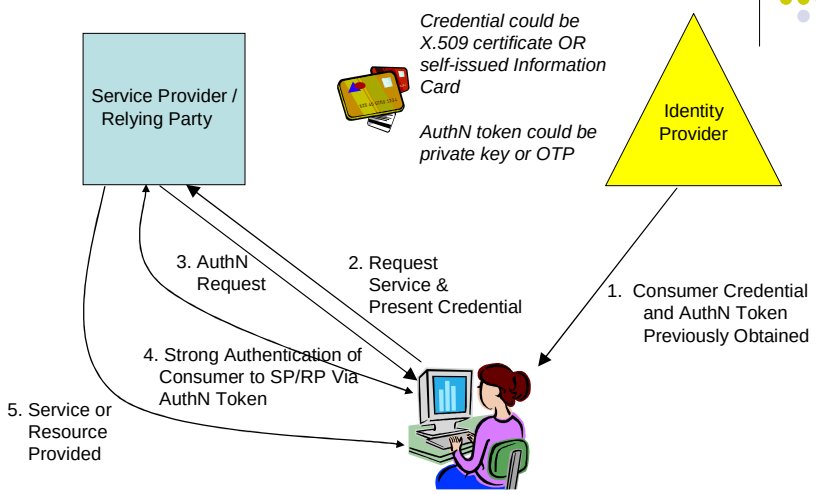
Open Issues in High Assurance Consumer Identity
Does a High Assurance Claim Always Require an Assertion from an Identity Provider?

- Yes, whenever an identity assertion or claim is needed:
  - Subject is unknown to Service Provider and seeks to establish a new high value, long-term relationship or account
  - Subject is unknown to Service Provider, seeks no long-term relationship but wants a high value, identity-dependent service
- BUT
  - The need for such claims is likely to be infrequent
  - An Identity Provider can become unavailable

Open Issues in High Assurance Consumer Identity
Does a High Assurance Claim Always Require an Assertion from an Identity Provider?

- Once a relationship/account is established, an authorization claim could be used to access or use the service.
  - Authorization claim/assertion from IdP based on authentication of consumer to the IdP via authN token **OR**
  - Localized challenge/response interaction between Service Provider and Consumer to demonstrate control of authN token.
- Since authZ claims are likely to be frequent, can the claim be authenticated without involving an IdP?
  - via PKI certificate or Information Card bound to the protected resource / account
  - Can U-Prove technology play a role?

Authentication of Authorization Claim
(Without IdP Assertions)



Open Issues in High Assurance Consumer Identity
Prevention of Identity Theft Based on Stolen PII

- Default assumption is that all SP/RPs should rely on a high assurance identity claim/assertion from a trusted IdP when establishing high-value, identity dependent relationships. BUT this won't happen for a while, if ever.
- In the meantime, if an IdP within some trust community has issued you a credential/token, how can you prevent someone who has stolen your personally identifiable information (PII) from claiming your identity?
  - Is there a way to discover if someone is using your PII?
- Possible role for Credit Reporting Agencies to notify credential holders when a SP requests a credit check based on PII for identification.

Open Issues in High Assurance Consumer Identity
Privacy

- What are privacy requirements regarding consumer information retained by, or gathered by, entities within the trust framework (IdPs, SPs/RPs)?
- How can high assurance identity assertions be limited to certain types of high value services involving financial transactions, access to healthcare records, etc?
  - Don't want to create a system whereby every Service Provider demands to know your identity

Open Issues in High Assurance Consumer Identity

Strategic Imperatives for Secure Cyber-Access (aTrust, Inc.)

1. Non-repudiable Internet access device authentication, (authenticating the Internet access device which is used to authenticate the human);
2. Non-repudiable Service Provider authentication which prevents phishing and man in the middle attacks;
3. Privacy compliant, non-repudiable, electronic human authentication that complies with Assurance Levels 1- 4 as defined in NIST SP 800-63;
4. Non-repudiable, authenticated (AL1-4) transaction confirmation and transaction authorization,
5. Non-repudiable, authenticated (AL1-4) business transaction identifier as required by (ISO 15944-eBusiness specs),
6. Non-repudiable authenticated (AL1-4) yes/no decision process to accept or reject a transaction.

kantara INITIATIVE

Open Issues in High Assurance Consumer Identity

Stakeholder Roles

Who are the stakeholders and how would they benefit from this?

- Service Providers in financial services, healthcare, etc.
- Financial and healthcare consortia
- Identity theft prevention and assistance organizations, as well as other consumer advocacy organizations
- Identity Providers
- Strong authentication vendors
- US Federal Trade Commission & other government agencies

CIWG Deliverables

Up to three individual ***KI Recommendations*** or ***CIWG Reports*** that together

- Reports on the current state of high assurance / strong authentication applications for consumers, and expands on the challenges and roadblocks that need to be overcome. [Phase 1]
- Recommends specific functions or capabilities of an identity infrastructure needed to support high assurance consumer claims that address the issues identified. [Phase 2a]
- Addresses feasibility issues and provides guidance for the widespread implementation and deployment ("rollout") of an identity infrastructure with these functions or capabilities. [Phase 2b]

Possible Additional Work
Phase 3

KI Recommendations or CIWG Reports (depending on interest and resources):

- Develop use cases or other guidance to demonstrate how technologies such as Information Cards, OpenID, U-Prove, etc., can be used to enable high-assurance identity claims for high value consumer transactions.
- Explore the feasibility of enabling consumers to discover and block attempts by unauthorized persons to use Consumer's personally identifying information (PII) to claim their identities for obtaining / accessing high value services.

Methodology

- Seek funding / resources for Phase 1, which consists of the report on the current state of strong consumer authentication.
- Based on Phase 1 results, determine the level of effort required to complete Phase 2, consisting of the recommendations and feasibility analysis. Seek funding / resources to complete Phase 2.
- If there is sufficient interest among potential funders, scope out Phase 3 and seek funding / resources.

Next Steps

- Amend the CIWG Charter to incorporate deliverable changes.
- Approach potential funders and other interested parties for the purpose of obtaining funding to support one or more individuals to begin work on Phase 1.
- Recruit volunteer CIWG participants and other subject matter experts willing to lend their expertise/opinions.

Appendix A

High Assurance Consumer Identity "Needs"

A Service Provider may have a need to establish, with a high degree of confidence, the identities of those consumers it forms relationships with, or at least other relevant personal characteristics or attributes of a particular consumer. Service Providers also have a need to keep unauthorized persons from accessing online accounts, records, and other resources that "belong" to consumers already known to the Service Provider. The consumer, on the other hand, has a need to ensure that others are not misusing his/her identity to establish these relationships, and that (unauthorized) others are not accessing the consumer's existing accounts/records/resources. A consumer may also have a need to obtain services that are dependent on certain personal characteristics or attributes, without having to reveal his/her identity to the Service Provider.

These two sets of needs (the consumer's need and the Service Provider's need) often go hand-in-hand, as illustrated in the following Consumer Identity Needs matrix. This matrix also shows that an Identity Assurance Framework can form the basis of an "authentication network" or federation to ensure that the consumer's need to prevent a misuse of his/her identity by others, as well as the Service Provider's need to know who it is dealing with, can be met.

Relationship Between Consumer Needs and Service Provider Needs

	Consumer's Identity "Needs"			
Service Provider's Identity Needs	Prevent others from using the consumer's identity to establish new accounts/relationships	Establish personal attributes w/o revealing identity to SP	Prevent unauthorized persons from gaining access to high value personal accounts, records, resources	Want only one or a small number of strong identity credentials; no "token necklace" problem
Establish a consumer's identity with high assurance	*Requires an Identity Provider that verifies consumer identities, issues "strong" credentials, and asserts verified identity claims*			*Need an Identity Assurance Framework to ensure trust between SP and IdP*
Establish other personal attributes about a consumer		*Requires an Identity Provider that verifies personal attributes, issues credentials, and asserts verified identity claims*		*Need an Identity Assurance Framework to ensure trust between SP and IdP*
Permit only authorized persons to gain access to high value services/accounts			*Requires a "strong" authentication token bound to consumer's account or data store*	*Need an Identity Assurance Framework to ensure trust between SP and IdP*
Efficient discovery of Identity Providers; no "NASCAR" problem	*Use a Selector/Active Client to display managed Information Cards associated with verified claims from IdPs*	*Use a Selector/Active Client to display managed Information Cards associated with verified claims from IdPs*	*Use a Selector/Active Client to display OpenIDs or Information Cards (managed or personal)*	*Need an Identity Assurance Framework PLUS Selector/Active Client*

At the intersection of each corresponding pair of consumer/Service Provider needs (shown in beige) is a requirement for functionality enabled by an Identity Assurance Framework. Each of these three sets of required functionality is described below as a separate scenario, and ensures that Service Providers can trust certain accredited Identity Providers to assert, with a high degree of confidence, the identities or authorization status of consumers seeking to obtain identity-dependent services.

In addition to the needs that consumers and Service Providers have for identity assurance, consumers don't necessarily want to be burdened with having to deal with numerous authentication devices or tokens to access all the accounts they have (the "token necklace" problem), and Service Providers don't want to deal with numerous and confusing options for determining which Identity Provider should be used to authenticate a particular consumer (the "NACAR" problem). One possible solution, noted in the yellow areas of the matrix, is to make use of graphical representations of consumer's digital identities as contained in "selectors" or "active clients.

Appendix B

Consumer Identity Scenarios

Several high-level scenarios are described in which identity-related claims of a consumer seeking to conduct a high value transaction online is important. This is important to the consumer so that potential fraudsters attempting to use the consumer's identity for such purposes can be thwarted, and is important to online service providers so they can be assured of the identity of a person seeking to establish a new, high-value relationship with it, or seeking to access existing accounts or resources.

Within each scenario are defined one or more use cases, which define specific instances of each scenario.

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 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 IdP**

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 IdP.
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 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 status 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 willing 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 Service Provider that allows the Service Provider to determine, with a high degree of confidence, whether this person is who he or 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 by NIST 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 wish to divulge his/her identity to the Service Provider.

Use Case 1: **Service Provider Initiates Request For a SAML Identity Assertion from a Trusted IdP**

Consumer has had his/her personal attributes verified by a trusted 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 IdP.
4. Consumer presents the credential to the Identity Provider (or the 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 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 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 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.

Appendix C

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.