




Identity Ecosystem Use Cases

AN IDESG STANDARDS COMMITTEE DELIVERABLE

Version 1.3
May 20, 2014

ABSTRACT



This document contains a set of use cases adopted by the IDESG to guide its work and for use by IDESG committees and stakeholders to inform their work efforts.

Table of Contents

1. INTRODUCTION	4
1.1 SCOPE	4
1.2 PURPOSE	4
1.3 DEFINITION	4
1.4 HISTORY	5
2. USE CASE PROCESS	6
2.1 USE CASE LIFE CYCLE	6
2.2 USE CASE WIKI	7
2.3 USE CASE CRITERIA	7
2.4 USE CASE LEVEL	8
2.5 USE CASE TEMPLATE	8
3. USE CASES	8
3.1 DEVICE INTEGRITY SUPPORTING USER AUTHENTICATION	9
GOALS / USER STORIES	10
ASSUMPTIONS	10
REQUIREMENTS	10
PROCESS FLOW	10
SUCCESS SCENARIO	11
ERROR CONDITIONS	12
REFERENCES AND CITATIONS	12
PRIVACY CONSIDERATIONS	13
USER EXPERIENCE/USABILITY CONSIDERATIONS	13
3.2 AUTHENTICATE PERSON USE CASE	13
3.3 IDENTITY PROOFING USE CASE	16
ACTORS	16
ASSUMPTIONS	16
PROCESS FLOW	16
SUCCESS SCENARIO	17
ERROR CONDITIONS	17
RELATIONSHIPS	17
REFERENCES AND CITATIONS	17
3.4 CRYPTOGRAPHIC AUTHENTICATION FOR ACCESS TO ONLINE RESOURCES	17
3.6 CREDENTIAL ISSUANCE USE CASE	27
3.7 ACCESS AGE RESTRICTED CONTENT USE CASE	29
3.8 PRIVACY ENHANCED BY USER AGENT	30
3.9 TRUST ELEVATION USE CASE	36
PRIVACY CONSIDERATIONS	41

3.11	UNSERVED AND UNDERSERVED PEOPLE USE CASE	42
3.12	SELECTIVELY DISCLOSE ATTRIBUTES USE CASE	45
3.13	REMOTE ELECTRONIC IDENTITY PROOFING USE CASE	48
ANNEX A – ACKNOWLEDGMENTS		53
ANNEX B – REFERENCES		54
ANNEX C – 2013 GOALS		55

1. Introduction

1.1 Scope

This document contains a set of Use Cases adopted by the Identity Ecosystem Steering Group (IDESG) intended to guide the many activities of the IDESG in its mission to cultivate and enhance the identity ecosystem and its underlying framework.

1.2 Purpose

The purpose of the IDESG Use Cases is multifaceted, but is primarily to inform and facilitate the work of the IDESG as a whole, by providing context for this work. In particular, the IDESG Use Cases are meant to:

- Frame the IDESG's initial objectives and scope of work
- Provide a basis for the development of IDESG work products
- Drive consensus among IDESG plenary members about the characteristics of the ecosystem and identity ecosystem framework they are trying to bring into existence
- Provide a method for the elicitation and capture the requirements of the various NSTIC constituencies
- Make more concrete the application of the National Strategy for Trusted IDs in Cyberspace (NSTIC) guiding principles in terms of real-world scenarios
- Serve as a test target against which IDESG work products can be evaluated
- Serve as a guide for the collective efforts of the IDESG, to maintain a common focus and alignment

These use cases are meant to describe digital identity problems to be solved and not to constrain solutions to these problems.

1.3 Definition

Use Cases are scenarios representing mission or stakeholder goals. It is a methodology used in system analysis to identify, clarify, and organize system requirements. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal.

According to Writing Effective Use Cases by Alistair Cockburn, a use case is explained as follows:

"A use case captures a contract between the stakeholders of a system about its behavior. The use case describes the system's behavior under various conditions as it responds to a request from one of the stakeholders, called the primary actor. The primary actor initiates an interaction with the system to accomplish some goal. The system responds, protecting the interests of all the stakeholders."

Different sequences of behavior, or scenarios, can unfold, depending on the particular requests made and conditions surrounding the requests. The use case collects together those different scenarios.”

1.4 History

Since the inception of the IDESG in August 2012, a need has been identified for a set of use cases to reflect the desired functionality and capabilities of the identity ecosystem. The Standards Coordinating Committee (SCC) was given the responsibility to facilitate this, as a collaborative effort across the IDESG. To this end, the SCC sponsored the IDESG Use Case Ad Hoc Group (UCAHG) in the fall of 2012 with a mission to gather use cases from IDESG members, review them for consistency and quality, present them to IDESG committees for comment, and recommend them to the SCC as candidates for adoption. A Use Case Wiki was set up and we began the collecting use cases from interested contributors in early 2013.

In spring 2013, as part of the IDESG plenary meeting, a Use Case Workshop was held with the goal of advancing the use case development activity, increasing IDESG involvement, and preparing for 2013 use case deliverables. At this workshop, a representative set of contributed use cases were analyzed by different functional group breakouts – privacy, security, standards, user experience, and economic inclusion which roughly map to the NSTIC Guiding Principles. The primary feedback from the workshop suggested the use cases should include less implementation or technology specific details.

2. Use Case Process

Development of use cases within the IDESG is meant to be a collaborative process involving all of the various committees, stakeholders and individuals comprising the organization. The SCC acts as the steward of this process and the UCAHG as the working group which operationalizes the process. Participation in the UCAHG is open to IDESG members and non-members and has actively solicited representation from all IDESG committees.

2.1 Use Case Life Cycle

The use case process is embodied within the adopted Use Case Life Cycle (UCLC) as shown in Figure 1.

Contributed	Working Draft	Committee Review	Compilation	Approval	Published
<ul style="list-style-type: none"> Initial base use case as submitted by a contributor and posted to the Use Case Wiki. Use cases may be in various stages of completeness and compliance, but must contain a title and brief description as a minimum. May be in use case template or free text “user stories”. 	<ul style="list-style-type: none"> In progress use case incorporating submitted contributions and comments as well as author extensions and enhancements. Working drafts will progress from “sketches” to relatively “complete.” During the course of refinement, drafts will migrate into template format. 	<ul style="list-style-type: none"> Mature use case. SCC reviews and coordinates review by other IDESG committees. SCC and IDESG comments incorporated. 	<ul style="list-style-type: none"> Sufficient number of candidate use cases are available. Diversity criteria applied. Individual use cases collected into a set (document). Privacy review conducted. 	<ul style="list-style-type: none"> Version to be balloted by the plenary. Comprises a set of use cases that have progressed through previous stages compiled into a deliverable document. Undergoes all MC and plenary approval processes as defined in the RoA. 	<ul style="list-style-type: none"> Approved IDESG work product. “IDESG Use Cases” Ready for use to inform other IDESG work.
<u>Progression gate:</u> <ul style="list-style-type: none"> Meets ‘relevance’ criteria 	<u>Progression gate:</u> <ul style="list-style-type: none"> Meets GP & ‘completeness’ criteria In template format AHG consensus to progress. AHG draft ready for committee review. 	<u>Progression gate:</u> <ul style="list-style-type: none"> All committee comments resolved. Meets all individual use case criteria. Committee draft becomes candidate for adoption. 	<u>Progression gate:</u> <ul style="list-style-type: none"> Set meets diversity criteria. Completed privacy review. SCC approves forwarding of work product for approval. 	<u>Progression gate:</u> <ul style="list-style-type: none"> Plenary ballot passes. 	<u>Progression gate:</u> <ul style="list-style-type: none"> N/A. May be appended by going through cycle again.
Individual/ AHG	Use Case AHG	Committees	SCC	MC/Plenary	IDESG

Figure 1. Use Case Life Cycle

To be published within this *IDESG Use Cases* document, a use case will have gone through the previous 5 steps as indicated above – from initial contribution through IDESG Plenary approval.

The use case process is iterative. After initial publication, additional sets of use cases are expected to be added to the document through a revision process. That is, additional sets having traversed the life cycle will be added to the document and the revised document submitted for Plenary approval. Additionally, existing use cases may be updated during the revision process as well.

The UCAHG maintains a queue of upcoming use cases for review, and accepts nominations from the Standards committee as input to that queue. The UCAHG will notify the Standards committee when the queue is short so that the Standards committee may call for nominations of additional use cases for review.

2.2 Use Case Wiki

IDESG Use Cases are collected and managed through the IDESG Use Case Wiki: https://www.idecosystem.org/wiki/Use_Cases. The Use Case Wiki contains all contributed use cases in various stages of completion with their current status indicated. Each use case includes a discussion page for the collection of comments on that use case.

2.3 Use Case Criteria

To progress through the UCLC, criteria are applied to each selected use case at various points. These criteria comprise the following:

Individual Use Case Criteria

- **Relevance**
 - Related to and supportive of the goals of the identity ecosystem
 - If "solved" would advance adoption of the identity ecosystem
- **Completeness**
 - Provide information that can be mapped to items of the template
- **Level**
 - Functional level which is not implementation specific
- **Guiding Principles**
 - How they address the four NSTIC guiding principles. In the spirit of the Cockburn explanation, the goal of the UCAHG has been to ensure that use cases generally capture and maintain the guiding principles of NSTIC in supporting solutions which are privacy-enhancing and voluntary, secure and resilient, interoperable, cost-effective and easy to use.

Criteria for Use Case Sets

- **Diversity**
 - As a set, cover a good-cross section of populations and functionality
 - Include edge cases; underserved communities
 - Address high, medium, and low risk scenarios
 - Focus on both the adoption of existing solutions as well as the creation of new capabilities

- Address the perspectives of all participants – RPs, IDPs, and end-users
- Address the range of identity life cycle functionality.

2.4 Use Case Level

After much discussion about the appropriate level of implementation specific details to allow in the final published use case, it was decided to follow the example of the OASIS Identity in the Cloud Use Cases. In this example implementation specific use cases have been allowed when they are clearly identified as such.

If a use case is too abstract, it provides little substance for analysis or application. Alternatively, if a use case is too implementation or technology specific, it becomes too laden with details and infinite variations are possible. This document aims to strike a balance between the two extremes.

2.5 Use Case Template

To ensure completeness and ease of use, use cases are formatted into a common template, consisting of the following elements:

- Use case description
- Actors
- Goals/user stories
- Assumptions
- Process flows
- Success scenario
- Error conditions
- Relationships
- References and citations

In addition, diagrams are encouraged and there are ancillary sections to address Guiding Principles considerations and domain expert considerations.

3. Use Cases

Use cases in this document are intended to be useful and illustrative, but not normative. The individual cases do not constitute an endorsement of a method, nor do they attempt to be comprehensive or purport to cover all important digital identity issues.

3.1 Device Integrity Supporting User Authentication

Use Case Description

Establish an integrity (aka health) claim for a device that together with other security measures, is good evidence of the integrity of the information exchanged with the user. Today many relying parties do ensure that users can only access their services with devices that are known to be in the possession of the user. This case extends that to allow the relying party to specifically request an integrity claim from the user's device.

Integrity has two meanings in computer security. The first relates to the device not having been changed in any way since it was created. The second relates to the device reliably behaving in an expected manner. In a modern operating system, with vulnerabilities patched every month, the former definition is not practical and so the later definition is the one that applies in this use case.

This use case distinguishes between two actors which are typically conflated in other use cases. The user is a carbon-based life form that has no innate capability to interface to any digital network. The user device is a silicon-based life form that is extremely good at interfacing to the digital networks at high speed, but communicates only a few bits per second to the user with a user experience that is often sub-optimal. For high value resources on the network, the resource owner would like to assure that the data once available on the user device is not leaked to unauthorized users. This is not possible if the resource owner (aka the relying party) does not trust the user's device's integrity with respect to confidential material placed on the device. There are other mechanisms to control data leakage, like remote device wipe, which are to be considered in other use cases.

Actors

1. Relying party (RP) in this case is a web service that requires user identity and other attribute information to complete a digital transaction.
2. Identity Provider (IdP) for this case contains identity of the user potentially with other attributes.
3. User Device is a modern computer system with graphical user interface and internet connectivity.
4. Device Attribute Provider (DAP) registers the user device, receives signed status information from the device, can evaluate the status of the device and generate an integrity claim for the device. This provider is called a Remote Attestation Service by some standards-making bodies.
5. Individual user in this case is a human being that wants to access a high value web site on the internet.

6. User agent is digital process running on a user device and trusted by a user to represent them to other parties in an ID ecosystem.

Goals / User Stories

1. The integrity of the device used for authentication of user identity provides the foundation for strong authentication and protection of user privacy.
2. RP can prove compliance with regulations that require proof of user intent.
3. User can know the device is only presenting the allowed information.
4. User identity theft from their personal device is blocked.

Assumptions

1. The RP has a relatively clear set of privacy compliance regulations to follow.
2. Users are provided sufficient motivation to acquire device integrity information to obtain web services.
3. Secure token services (STS) are available in the marketplace to provide user ID (IdP) and device integrity (DAP).

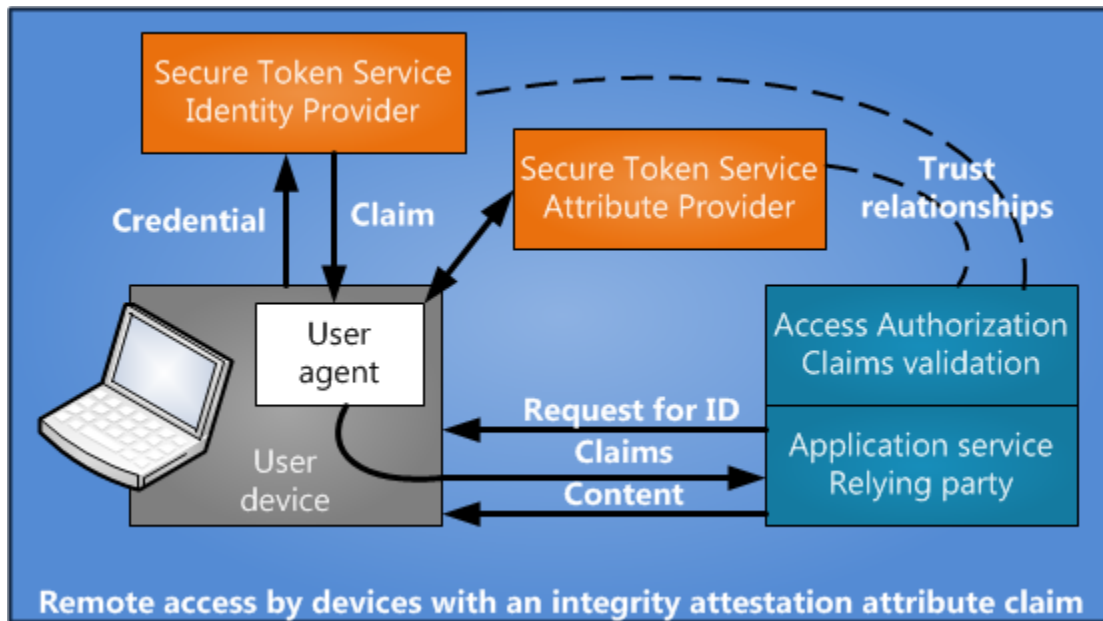
Requirements

1. Individual users have access to a modern digital device with secure root of trust.
2. A minimalist standard taxonomy of data type is presented for user choice.
3. The user device is able to collect credentials from the user and transmit them to the identity provider.
4. Claims from the identity provider and attribute providers, including the device attribute provider, can be composed into a bag of claims to be sent to the relying party. In this case the compositing function is provided by the user device.

Process Flow

1. The user establishes an account with one or more IdPs.
2. The user's device is registered with a device attribute provider.
3. The user accesses a web site which requires identity attributes of some sort to continue to process the user request. That web site then becomes a relying party.
4. The RP uses a standard protocol and taxonomy to request the information needed from the user.
5. This request for information is intercepted by an agent for the user that can:
 - Determine if the requested information is available,
 - Determine if the user has already authorized release of the requested information to this RP,
 - Display any remaining choices to the user to acquire more attributes or release those already available,

- Compose user and device claims in a way the RP can evaluate the data,
- Send the composed claims to the RP who has sole responsibility to determine if sufficient identity and attribute information has been proved to provide the requested access.
- Repeat these steps until the RP is satisfied or one side gives up and abandons the effort.



1. The above figure shows the user agent as a part of the user device. Other implementations are certainly possible. It is responsible for collecting, storing and releasing a collection of claims to the relying party based on informed user consent.
2. The Secure Token Service / Device Attribute Provider is called a remote attestation service in some environments. It accepts the information created by the device at boot time in a Trusted Platform Module (TPM) to compare with known good configuration information to attest to the integrity (health) of the device by means of a device attribute claim.

Success Scenario

1. Strong authentication using two factors: user ID plus machine integrity claims. This improves the security of users on the internet.
2. Modern devices in common use for connecting users to the internet already come with a hardware root of trust that can be used to report on the current status of the device in a way that is not susceptible to tampering.
3. A device integrity attestation attribute service becomes available in the cloud to the user at little cost to create claims as to the integrity of the user device and to enable

easy remediation of defects found in the device integrity. This service acts like an extension of an antivirus product that be determined if the device is truthfully representing its status.

4. The RP gets access to the user identity and device integrity information in claims that are trusted to authorize release of the desired information to the user.

Error Conditions

1. User does not have the credentials required by the relying party. To mitigate this condition, the relying party redirects the user to one or more sources of appropriate credentials.
2. The device or user agent loses the trust of the Registration Authority (RA) and hence of the RP. To mitigate this risk, the user must be given actionable steps to get their devices and agents back into compliance. It should never be the case that an “unauthorized” message be transmitted without mitigation steps.

References and Citations

1. Privacy Enhancing Technologies are outlined in a companion use case https://www.idecosystem.org/wiki/Privacy_Enhancing_Technologies, which shows various ways to hide the identities of the user and the user device.
2. Authenticate Windows Azure with ADFS at <http://technet.microsoft.com/en-us/magazine/dn250023.aspx>
3. Trusted Platform Module at http://www.trustedcomputinggroup.org/developers/trusted_platform_module/specifications
4. Endpoint Compliance Profile at http://www.trustedcomputinggroup.org/resources/tnc_endpoint_compliance_profilespecification
5. NIST SP 800-164 Hardware-Rooted Security in Mobile Devices at http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
6. Cloud Platform Audit and Asset Management using Hardware-based Identities at <http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html#Toc324801965>. This Oasis developed use case describes the companion problem of establishing trust in a cloud provider using a virtual machine environment. The use is very detailed and provides two relevant comparisons to the present use case. First, the devices now in development for users often are enabled on virtual machine technology and so can help with the implementation of device integrity of the user device. Second providers of identity and attribute data could directly use the Oasis use case to provide proof of their integrity to both the user and to the relying party.

Privacy Considerations

A privacy implication occurs when raw device data is transferred instead of just claim information. For example, this could be through the public key in the integrity certificate. In many cases the device is used by one or a small number of users which would allow linkage of this attribute to a user. Like any attribute, the device integrity claim would only be provided if the user authorized its release. It is certainly also possible to use a privacy enhancing technology provider (PETP) to combine all proffered claims into a composite claim with some identity that cannot be linked back to the original user. Where comparison of the device configuration occurs should be considered. Comparisons performed at the attribute provider could provoke a privacy concern.

User Experience/Usability Considerations

Existing device integrity solutions require direct involvement of the user in the process of establishing a connection to a Device Attribute Provider. The process must be made easier before a user is likely to expend the time or money to create integrity claims for their personal devices. The most natural way to establish this integrity claim is to make it a part of the Anti-malware software installation which many users have enabled.

The best way to motivate the users to maintain the security and integrity of their devices is by monetary incentives or enhanced convenience. This is typically only possible for high value content like current movies or sensitive enterprise data that is only released to devices with known integrity.

3.2 Authenticate Person Use Case

Use Case Description

A user seeks to gain access to an online resource that requires authentication, and that user becomes the Claimant actor. The online resource provides the Claimant the ability to authenticate their identity using an Identity Service Provider of the Claimant's choice through the use of privacy enabling and standards based protocols.

Actors

1. Claimant – wants to obtain access to a web resource
2. Identity Service Provider – performs primary authentication of the Claimant's credentials
3. Relying Party – requires a level of assurance about the identity of the Claimant

4. User Agent – accepts user input from the Claimant and mediates the authentication process

Goals / User Stories

The Claimant is able to gain authenticated access to the Relying Party online resource without having to provide the Relying Party with a primary credential. The Claimant is able to perform a single authentication with an Identity Service Provider of their choice and the manner in which the Identity Service Provider is identified is an intuitive process. An example, but not a requirement, of an intuitive process would be to identify the Identity Service Provider via the Claimant's email address. If the Claimant had previously established a trusted relationship with the Identity Service Provider, then a session management design should enable the authentication to take place without requiring an additional prompt for the primary credential.

Assumptions

It is assumed that the Claimant has already been identity proofed to some LOA (Level of Assurance), and has already received credentials binding their identity to one or more tokens.

Requirements

1. The Claimant must be capable of selecting an Identity Service Provider of their choice (provided that the Identity Service Provider meets the LOA requirements of the Relying Party)
2. The Identity Service Provider must present the Claimant with privacy protection choices that minimally include the ability to not disclose their true identity (e.g. use a pseudonym)
3. The Identity Service Provider must present the Claimant with an option to not track the Relying Party

Process Flow

1. The user attempts to access a resource and the site require an authenticated identity in order to proceed.
2. The Claimant is able to intuitively indicate to the Relying Party their preferred Identity Service Provider
3. The Relying Party directs the Claimant to their Identity Service Provider via a User Agent, e.g. a web browser
4. The Identity Service Provider authenticates the Claimant. The Identity Service Provider may accomplish this authentication either via performing primary authentication of the Claimant, or via the Claimant's possession of a bearer token showing that authentication has already taken place, e.g. via the presentation of a session or persistent cookie. Some Relying Parties may have differing requirements that dictate whether or not cookies or other session tokens may be used, and if so what lifetime is acceptable.

5. Upon successful authentication of the Claimant, the Identity Service Provider generates an Identity Token which contains the claimed identity of the Claimant and possibly other personally identifiable information. The Claimant must be able to indicate what personally identifiable information (PII) is included in the Identity Token, including the usage of real name vs. pseudonym or other personally identifiable information such as email address, street address, or birthday. The Identity Token is sent back to the Relying Party via the Claimant's User Agent.
6. The Relying Party validates the Identity Token from the Identity Service Provider and extracts the claimed identity and possibly other personally identifiable information. The Relying Party may optionally query a third party attribute provider for additional attributes bound to the claimed identity or may map the claimed identity to local attributes.
7. The Relying Party makes authorization decisions based on the claimed identity, attributes of the identity, or both, and when applicable returns resource to the Claimant's User Agent.

Success Scenario

The Relying Party returns the requested resource to the Claimant's User Agent.

Error Conditions

1. Relying Party cannot validate assertion.
2. Identity Service Provider cannot authenticate the Claimant.
3. The Relying Party rejects the LOA of the Identity Token.
4. The Relying Party is unable to authorize the Claimant even after validating the claimed identity.
5. The Claimant is not authorized to access the requested application, resource or service.

Relationships

Extended by: Authenticate Using Pseudonymous Identity Use Case

References and Citations

- NIST SP 800-63-1

Privacy Considerations

As currently constructed, this use case adopts the NIST SP 800-63 model of identity providers rather than the separate Identity Provider/Attribute Provider described in the NSTIC strategy. Accordingly, it uses the concept of Level of Assurance that includes both the strength of authentication and the confidence in certain identifying attributes such as name. Therefore, it does not support strong authentication in the absence of identifying attributes, such as the ability to assert one's age without identifying oneself in an attributable way. (See NSTIC

strategy, page 11). Identity proofing relates to the binding of certain attributes to the identity, and therefore is maintained by an attribute provider, and is related to attribute release, not authentication *per se*.

Authentication of a person can release as little as an identifier, which may or may not be persistent from one session to the next. Accordingly, the use case does not address authentication for *anonymous or pseudonymous interactions*, which are considered important capabilities in the NSTIC. Pseudonyms used at multiple parties may allow tracking. In both cases, trustable assertions from an attribute provider might be provided following authentication, even in the absence of a persistent identifier (in the anonymous case) or attributes that are intended to allow inference of the entity associated with those attributes. Use of email address may be considered by some to not be privacy preserving.

3.3 Identity Proofing Use Case

Identity Proofing is the process by which a Credential Service Provider (CSP) and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. This verification can be in-person or remote.

Actors

1. Credential Service Provider
2. Registration Authority
3. Applicant

Assumptions

1. There is verifiable information about Applicant that Registration Authority can validate.
2. Registration Authority has access to authoritative sources of attribute verification.

Process Flow

1. Applicant presents an identity claim to the Registration Authority. This identity claim consists of a set of attributes that Applicant asserts belong to them. These attributes can include legal name, date of birth, address of record, etc. During in person identity proofing, evidence can consist of documents that support the identity claim. During remote identity proofing, evidence is supplied by the applicant to substantiate that the claimed identity belongs to the Applicant.
2. Registration Authority validates the claimed identity by checking the attribute claims against authoritative sources of attribute information.

Success Scenario

Identity Proofing completes successfully when the Registration Authority accepts or rejects the applicant's identity claim.

Error Conditions

1. Applicant does not have address of record.
2. Applicant cannot supply verifiable attributes.
3. Registration Authority's verification processes fails.

Relationships

Extended by: Remote Identity Proofing Use Case, In-person Identity Proofing Use Case

References and Citations

- NIST_SP_800-63-1

3.4 Cryptographic Authentication for Access to Online Resources

Use Case Description

This use case outlines two approaches for providing cryptographic authentication to online resources. In both approaches, the need for shared secrets between users and relying parties, such as passwords or answers to challenge questions, is eliminated.

One of the NSTIC Guiding Principles is that identity solutions should be secure and resilient. Authentication methods that rely on shared secrets, such as passwords, are well known to be less secure than methods based on public key cryptography. NSTIC-compliant identity solutions for high assurance applications such as access to high value online resources, should therefore eliminate reliance on weak authentication methods based on shared secrets. The NSTIC derived requirements compiled by the National Program Office also specify that identity credentials should be resistant to theft, tampering, counterfeiting, and exploitation. Although no single authentication technology has a monopoly on these properties, public key cryptography arguably provides better security than most current alternatives. In addition, recent advances have the potential to make public key crypto (cryptography) usable for consumer applications. Although a use case does not need to focus on any specific technologies, a goal of this use case is to help ensure that an NSTIC-compliant identity ecosystem will incorporate strong authentication methods that have previously not been usable by consumers.

Actors

1. User: An individual who needs to access an online resource.
2. Token: Something that a user possesses and controls that is used to authenticate the user for access to a protected resource such as a financial account.
3. Public / Private Key Pair: a public cryptographic key and its corresponding private key. The private key resides on the user's computing device or external USB device or smartcard, and can be locked with a PIN or password. The private key acts as a token.
4. Relying Party: a website that must authenticate a user for access to a service or resource provided by the relying party.
5. Device: a computing device such as a personal computer, laptop computer, tablet computer, or mobile phone that is able to store and manipulate cryptographic keys. It could possibly also include USB dongles that include processing capabilities, as well as smartcards.
6. Third Party: a third party entity that can provision private / public key pairs on a user's device, and can provide an additional layer of security by acting to sign an authentication request independently of the user.

Goals / User Stories

The goal of this use case is to outline two approaches for providing cryptographic authentication to online resources. In both approaches, the need for shared secrets between users and relying parties, such as passwords or answers to challenge questions is eliminated. The term "cryptographic authentication" here means that a relying party is able to authenticate a user seeking access to an online resource by means of an authentication protocol that verifies that the user controls a cryptographic private key. It is assumed that the corresponding public key has been previously bound to the online resource.

Neither of these two approaches depends on the use of client-side certificates issued by a certificate authority that has vetted the user's identity prior to issuing the certificate. Instead, it assumes the service provider/relying party has independently determined a particular user is entitled to access an online resource, and is able to bind a public cryptographic key to that resource.

In one approach, the relying party directly provisions a private/public key pair on the user's device, uploads the public key to the relying party site, and binds the public key to the online resource. Ongoing authentication for access to the resource then depends on a user being able to demonstrate control of the associated private key.

An alternate approach assumes the existence of a third party entity that provisions public/private key pairs on the user's device, and provides an additional measure of security by means of an authentication protocol that requires the third party to demonstrate control of an additional private key.

Traditional Public Key Infrastructure (PKI) and client-side certificates also achieve the goal of providing strong cryptographic authentication. But PKI and client-side certificates have been cumbersome and costly to deploy and maintain, and are not widely used especially for authentication of consumers. This use case proposes an alternative to traditional PKI in which public/private key pairs are provisioned directly on user devices without involvement of client-side certificates or certificate authorities.

Assumptions

Strong authentication for access to online resources is assumed to require two-factor authentication, where the two factors are "something you know" and "something you have."

The "something you have" factor consists of a computing device, such as a desktop or laptop PC, tablet computer or Smartphone, is used to access a protected online resource. It could possibly also include a separate authentication device that is able to store and manipulate private keys. To transform a computing device into a secure authentication token, a public/private cryptographic key pair will be provisioned on the user's device. The public key will be uploaded to the relying party site, and strong authentication will depend on the user's ability to demonstrate control of the private key.

A private key on the user's computing device may be locked, and is only usable for authentication if it can be unlocked with a PIN, password, or biometric. This PIN or password is the "something you know" authentication factor, while a biometric is a "something you are" authentication factor. However, none of these is a shared secret between the user and the relying party because neither the PIN, password nor biometric information leave the user's device.

In the case where the relying party directly provisions a public/private key pair on the user's device, an appropriate application will exist on the user's device to manage multiple private keys that are used for authentication to multiple websites. This application may consist of a browser plug-in or extension, and must provide a user interface that makes it easy for users to cryptographically authenticate to different relying party sites. Each user device will be

provisioned with its own public/private key pair specific to that device, and each relying party site will need to maintain public keys for each of the user's devices.

A mechanism will exist for users to add new devices and to provision those devices with appropriate public / private key pairs so that those devices can be used for authentication to protected resources at a relying party site. A similar mechanism can exist to remove a device.

In the case where a third party is used to provision public/private key pairs on the user's device(s), an additional private key maintained by the third party is used in the authentication protocol. An advantage of this approach is that if a device is lost, the user can instruct the third party not to sign an access request with its private key originating from the lost device. On the other hand, involvement by a third party introduces the possibility that the third party may be unavailable during the authentication process, rendering the user unable to authenticate to the relying party site.

User's computing devices must be equipped with an application that provides users with the ability to easily manage multiple crypto private keys for authentication to multiple websites.

Process Flow

1. Enrollment

When a new user is enrolled at a relying party site, the site instructs the user's device (browser) to generate a public /private key pair. The device-specific public key is uploaded to the relying party site, along with some type of user and/or device identifier. This public key is bound to the user's protected resource at that site.

Alternately, when a third party is involved, the device public key along with the public key of the third party are both uploaded to the relying party site, and bound to the protected resource.

2. Authentication for Access to a Protected Resource

The relying party site (or the app on the user's device) will display a button for the user to click for access. The relying party site identifies the user and/or device on the basis of some type of user / device identifier, and sends a challenge to the user's device. The user clicks on the button, and is prompted for a PIN or password to unlock the corresponding private key on the user's device (if the key was previously locked). Once unlocked, the private key is used to digitally sign a response, which is returned to the relying party. The relying party verifies the

digital signature with the corresponding public key. If verified, the user is allowed to access the protected resource.

Alternately, if a third party is used, the response to the relying party's challenge is signed by the private key on the user's device, and is then forwarded to the third party. After authenticating the device using the device's public key, the third party signs the response with the third party's private key, and then returns it to the user. The user forwards the doubly-signed response to the relying party. The relying party verifies the two digital signatures with the public keys corresponding to the user's device and the third party.

3. Authentication of an Individual Transaction

When a user initiates a specific type of transaction, such as moving money out of a financial account, the user's device may sign the transaction with the device's private key. The relying party site verifies the signature with device's public key. Alternately, the third party private key is also used to sign the transaction.

4. Adding a New Device

A user will be able to provision new public / private key pairs on a new device by leveraging the capabilities of an existing device that has already been provisioned with key pairs for multiple relying party sites. One possible way to do this may be for the user to activate a process on the existing device that causes an email to be sent to the user, which contains a link that must be activated on the new device. Once activated, this link generates a private / public key pair on the device. For added security, the user may be required to enter a one-time code sent to the user's out-of-band mobile phone.

Success Scenario

1. Users are successfully provisioned with public / private key pairs on each of their computing devices, for strong authentication to relying party websites.
2. Users are able to successfully authenticate to each relying party website where they have protected resources, using strong cryptographic authentication.
3. Users can successfully add new devices for strong authentication to their protected resources, and remove them if necessary.

Error Conditions

1. Relying party sites do not support this use case.
2. There are difficulties or errors when provisioning the necessary public/private key pairs on user's devices.
3. Users cannot successfully add a new device (or remove an existing device) for access to a relying party site.

4. If a third party is used for added security, the third party may be unavailable to sign a response or transaction with its private key when needed.

Relationships

1. Two other consumer-class use cases rely on public key cryptography for user authentication. These are: IRS Identity Theft Use Case and Delegated Authentication for User Managed Access Use Case.
2. This use case extends the Authenticate Person use case.

References and Citations

- In addition, other initiatives and commercial products exist that are geared to making public key cryptography usable for consumer-class applications. These include the FIDO Alliance's Universal Second Factor (U2F) Initiative, as well as OneID.

Privacy Considerations

Privacy issues may arise if the Third Party has associated knowledge of the users activity or if the Relying Party is able to associate the user with a given Third Party. Key management should be mechanized so that unintended trackability and Man in the Middle (MITM) attacks can be avoided.

3.5 Delegated Authentication for User Managed Access

Use Case Description

There are many instances in which the owner of an online protected resource, such as a bank account, health record, or other information repository, needs to allow someone else to access the resource. Since many, if not most, online resources today are protected with only a password or other shared secret(s), the simplest way in which a resource owner can allow someone else to access the protected resource is to share knowledge of the same user ID and password that the resource owner uses. But in addition to being insecure, this method provides the other party with unconstrained access to the protected resource.

However, it is often the case that the resource owner can identify a specific set of individuals or entities that should have access to the resource. Specifically, this use case proposes an authentication scheme that uses a private cryptographic key residing on the requesting party's computing device as a second "something you have" authentication factor. In order to provision a public / private key pair on an authorized requesting party's device, this use case requires that the requesting party be able to enter the URL of the Authorization Server on the

device, and that a one-time code be sent to the requesting party's mobile phone, which will then be entered on the device where the key pair will be provisioned.

Even if the specific set of individuals authorized for access to the protected resource do have relationships with third parties that could issue trusted claims, there is potential value in enabling the requesting party to directly authenticate to the Authorization Server using a strong authentication token, without a third party needing to be involved in the transaction. By eliminating the participation of a third party in every authentication transaction, a potential privacy issue is eliminated. A potential reliability issue is also eliminated, since the unavailability of the third party to issue a claim to the Authorization Server would imply that the requesting party would not be able to access the protected resource.

One of the NSTIC Guiding Principles is that identity solutions should be secure and resilient. Authentication methods that rely on shared secrets, such as passwords, are well known to be less secure than methods based on public key cryptography, for example. NSTIC-compliant identity solutions for high assurance applications, such as a user allowing someone else to have restricted access to the user's high value online resources, should strive to eliminate reliance on weak authentication methods based on shared secrets whenever possible. The NSTIC derived requirements compiled by the National Program Office also specify that identity credentials should be resistant to theft, tampering, counterfeiting, and exploitation. Although no single authentication technology has a monopoly on these properties, public key cryptography arguably provides better security than most, if not all, current alternatives. In addition, recent advances have the potential to make public key crypto usable for consumer applications. Although a use case does not need to focus on any specific technologies, a goal of this use case is to help ensure that an NSTIC-compliant identity ecosystem will incorporate strong authentication methods that have previously not been usable by consumers.

Actors

1. A Resource Owner is the owner of a protected online resource who wishes to allow another individual to have access to that resource.
2. A Requesting Party is an individual person who seeks access to a protected resource owned by the Resource Owner.
3. An Authorization Server is an online system that allows the Resource Owner to specify a set of access permissions to be granted to the Requesting Party. The Resource Owner interacts with the Authorization Server to specify the policies or constraints that define the permissions that will be granted to a particular Requesting Party. The Resource Owner may choose to provide full access to the protected resource, so that the Requesting Party is treated the same as the Resource Owner when accessing the

resource. Alternately, the Resource Owner may choose to specify a limited, constrained set of permissions.

4. A Resource Server is an online system that a Requesting Party interacts with in order to obtain access to the protected resource. The Requesting Party must authenticate to the Resource Server to gain access to the protected resource.

Goal/User stories

There is increasing recognition that resource owners need to have a way to delegate access to protected resources that is constrained in some way, as determined by policies defined by the resource owner. This need is at the heart of the Kantara Initiative's User Managed Access (UMA) project. UMA is based on claims-based access control, which means that entities entitled to access protected resources will be given permission to do so contingent upon presentation to an Authorization Manager of an appropriate "claim." A claim consists of a relevant set of attribute values pertaining to the requesting party, which is the entity that is requesting access to the resource. The idea is that an arbitrary requesting party may gain access to the protected resource, according to a predefined set of "permissions", provided that the claims satisfy some criteria designated by the resource owner. Hence it is not necessary for the resource owner to be able to designate specific individuals or entities authorized to access the resource. UMA does not specify a particular method for these claims to be generated. However, to access high value resources, presumably the resource owner will require some sort of trusted third party to verify a claim rather than allow a requesting party to issue self-asserted claims. This requires that requesting parties seeking access to high value resources have a relationship with such a third party, and that the requesting party is able to authenticate to the third party prior to the claims being generated. Authentication in this case should require a stronger authentication token than a static password. The use of public key cryptography for providing strong authentication, as described in the use case Cryptographic Authentication for Access to Online Resources, is a viable alternative.

Assumptions

Resource Owners are able to specify a given set of individuals who are authorized to access a protected resource according to permissions set by the Resource Owner.

An NSTIC-compliant identity ecosystem is presumed to incorporate functionality necessary to make public key cryptography usable and practical as a strong authentication method for consumer applications such as UMA.

An appropriate application (the "crypto manager") will exist on the Requesting Party's device to generate and manage public/private key pairs for authentication to multiple websites. This application must provide a user interface that makes it easy for users to cryptographically authenticate to multiple websites. This crypto manager is assumed to be

an important component of NSTIC-compliant identity ecosystems and will be deployed on user devices in a manner yet to be described.

For increased security, Requesting Parties will only be able to access protected resources from “registered” devices, where a device becomes registered if it is provisioned with a private crypto key providing strong authentication. The registration process itself requires that the Requesting Party control a particular email account as well as a particular mobile phone number.

A Resource Owner is able to successfully create a policy specifying the constraints under which a Requesting Party is given permission to access a protected resource.

Process Flow

Resource Owner

The Resource Owner logs in to the Authorization Server to either define a new policy that specifies the access permissions for some specific Requesting Party, or to reuse a previously-defined policy to assign access permissions for the Requesting Party. The method of authentication used by the Resource Owner for this purpose is not specified here.

After the access permissions are defined, the Authorization Server requests that the Resource Owner provide a mobile phone number and email address for the Requesting Party. It is important to note that if the Requesting Party cannot receive SMS text messages on a mobile phone, the Resource Owner must indicate this and provide the phone number of a device that can receive ordinary voice calls instead.

After this information is provided, the Authorization Server sends an email message to the Requesting Party containing the URL of the Resource Server, together with a unique permission code. The message instructs the Requesting Party to register the device(s) that the Requesting Party wishes to use to access the protected resource by: (a) browsing to the URL of the Resource Server using the desired device, (b) providing the permission code to the Resource Server registration page, (c) receiving a one-time code from the Requesting Party’s mobile phone, and (d) entering it on the Resource Server registration page. If the Requesting Party does not use a mobile phone that can accept SMS text messages, the alternative is that the Resource Server makes an automatic call to the Requesting Party’s phone, and generates a spoken one-time code.

To change the access permissions granted to the Requesting Party, including revocation of the permissions, the Resource Owner logs in to the Authorization Server, using the permission

code to identify the set of permissions to be changed. Once changed, the new set of permissions is associated with the permission code.

Requesting Party

The Requesting Party receives an email from the Authorization Server, and proceeds to register a desired device for access to the protected resource, as described above.

As part of the registration process, a private cryptographic key is provisioned on the Requesting Party's device (using the crypto manager), with the corresponding public key sent to the Resource Server. The private key, in combination with the permission code, will allow the Requesting Party to access the protected resource with the appropriate permissions. An additional option may require the Requesting Party to provide a PIN or password to unlock the private key on the device. However, this PIN/password is not a shared secret, since it never leaves the device.

Once registered, the crypto manager on the device will presents a simple user interface when the Requesting Party accesses the appropriate Resource Server access page. The Requesting Party clicks a button to initiate the cryptographic authentication process, which may require the Requesting Party to provide a PIN or password to unlock the private key. Once this is done, the Requesting Party is granted permission access to the protected resource.

Any changes to the access permissions made by the Resource Owner will be noticed when the Requesting Party authenticates to the Resource Server and seeks to access the protected resource, since the modified permissions are associated with the same permission code used during the authentication process.

Success Scenario

- The Requesting Party is able to obtain access to the protected resource after a successful challenge-response interaction between the Resource Server and the Requesting Party's device that depends on the presence of the private key provisioned during the registration process
- All interactions successfully conform to a common policy.

Error Conditions

- The registration process is compromised in some way, so that an attacker is able to register his device for access to the protected resource.
- A hacker is able to compromise the private key on the Requesting Party's device.

Privacy Considerations

Implementation details such as who should operate the authorization server should be considered. In addition, due diligence should be performed when considering the use case participants ability to track user activity.

References and Citations

- Cryptographic Authentication for Access to Online Resources Use Case
- Eve Maler: Two Step Verification Will End Consensual Impersonation (http://blogs.forrester.com/eve_maler/13-04-01-two_step_verification_will_end_consensual_impersonation)
- Kantara User Managed Access (UMA), <https://kantarainitiative.org/confluence/display/uma/Home>

3.6 Credential Issuance Use Case

Use Case Description

The use case pertains to the issuance of a credential during the registration process, after identity proofing has optionally occurred. Below are some non-normative examples of issuance of particular forms of authentication factors for credentials.

Example: Linux passwords

On Linux systems passwords are selected by the Claimant and a hash of the password is recorded in /etc. /password associated with the Claimant's username.

Example: Asymmetric Cryptography

Asymmetric cryptography with user-generated keys allows the CSP to record the public key of the Claimant without having knowledge of the associate private key. In a PKI model, the CSP can issue X.509 certificates that associate the public key with the Claimant's unique identifier; alternatively in a non-PKI model, the CSP can record the Claimant's public keys in a trusted identity store associated with the Claimant's unique identifiers.

Example: One Time Password (OTP) to Mobile Phone

Authentication tokens based on sending One Time Passwords (OTP) to a mobile device, so credentials might consist of mobile phone numbers associated with the Claimant's unique identifier.

Actors

1. Entity (a Person or Non-Person Entity) has enrolled for credentials from Credential Service Provider
2. Credential Service Provider has the goal of issuing credentials to Entity.
3. Registration Authority provides verified information about an entity so as to issue credentials.
4. Applicant or Sponsor presents verifiable information about the entity in order to obtain credentials.

Assumptions

1. The Registration Authority can provide verified identity attributes for the Entity.
2. Credentials consist of one or more authentication factors linked to the Claimant's unique identifier.

Process Flow

1. In the case of credential issuance to a Person, the Claimant is the Person to whom credentials are being issued. In the case of credential issuance to the Non Person Entity (NPE), the Claimant is the NPE and the Sponsor is the individual requesting credentials on behalf of the NPE. The process flow sometimes refers to Claimant/Sponsor which indicates the human in the process.
2. During the credential issuance process, each authentication factor must be collected or generated and recorded in such a way as to support subsequent authentication operations.
3. When a sufficient number of authentication tokens have been generated and recorded, the Credential Issuance process is complete and the Applicant becomes a Subscriber.

Note: The credential issuance process may require publication of information.

Success Scenario

1. All authentication tokens are successfully generated.

Error Conditions

1. An authentication token cannot be generated
2. Storage of authentication factor information fails.

Relationships

1. Related to: Identity Proofing Use Case, Authenticate Person Use Case

References and Citations

- NIST Special Publication 800-63

Privacy Considerations

User knowledge with regard to what information is contained in the credential and how that information is released should be communicated to the user. Other implementation considerations should be explored to prevent correlation of user data among applicable parties to the transaction.

3.7 Access Age Restricted Content Use Case

Use Case Description

Enable individuals to prove that they are within a certain age range without disclosing their identity. This could support Children's Online Privacy Protection Act (COPPA) safe harbor provisions by verifying minority status without identification, or to enable adults to access mature content with privacy.

Actors

1. Subscriber is a human wishing to access a service with age restrictions without revealing their identity.
2. Service Provider needs to provide access only to individuals within a specified age range.
3. Attribute Provider provides an age verification service.

Goals / User Stories

1. Enable individuals to prove that they are within a certain age range without disclosing their identity.
2. No identity information about adult must be verifiable but age.

Assumptions

1. Individuals are willing to share identity information with Attribute Provider in order to obtain anonymous age verified access to Service Provider.

Process Flow

Proof of Age Process Flow

1. Subscriber enrolls with Attribute Provider
2. During enrolment, Subscriber undergoes Identity Proofing that includes verification of their Date of Birth.
3. Attribute Provider and Subscriber establish an anonymous credential by which Subscriber can authenticate to Attribute Provider.

Verification of Age Process Flow

1. Subscriber attempts to access an age-restricted Service Provider.
2. Service Provider discovers Attribute Provider.
3. Subscriber informs Service Provider of Attribute Provider, or
4. Service Provider queries for Attribute Provider that can verify Subscriber.
5. Service Provider informs Attribute Provider of required age range.
6. Subscriber authenticates to Attribute Provider.
7. Attribute Provider locates Subscriber's Date of Birth and calculates whether Subscriber is in the required age range.
8. Attribute Provider responds to Service Provider with confirmation or denial that the Subscriber falls in the required age range.

Success Scenario

1. The use case is successful when the Service Provider can verify whether Subscribers are in the specified age range.

Failure Scenario

1. Service Provider is unable to find an Attribute Provider to vouch for the Subscriber's age.

Error Conditions

1. Adult viewing laws in various states or countries conflict resulting in a false positive.

Relationships

1. Related to Identity Proofing Use Case, Verify Identity Claim Use Case

References and Citations

1. NSTIC Strategy (p. 2, p. 11, p. 23, p. 38)
2. Children's Online Privacy Protection Act (COPPA)

3.8 Privacy Enhanced by User Agent

Use Case Description

Provide sufficient claims to a relying party to allow an online transaction to commence while limiting disclosures to those attributes that the user is willing to share with that party. A user agent is present in all digital transactions to represent a legal entity, the user, to the digital world. Enabling privacy in the digital world requires the existence of a Privacy Enhancing Technology Provider which can exist either as a part of the user agent or in some cloud service. This use case considers the former implementation. In either implementation there will be an actor that accepts claims from a variety of sources and a set of privacy policy directives from the user to craft a set of claims for the relying party that is designed specifically to meet both

the requirements of the relying party and the user's privacy directives. It is important that both the user and the relying party trust the user agent. In this case a registration authority is described as the means for either to trust the user agent. As always the relying party has the final say on whether the proffered claims are adequate to allow the transaction to continue.

Actors

1. User: In this case a human being who wants to access services of a relying party and still retain privacy for details not needed by the RP.
2. Device Owner: An entity that can set privacy policy on the user agent residing in the user device. In this case, the user will be the owner of consumer devices. For enterprise owned devices, the owner may place restrictions on enterprise-owned data over and above user privacy concerns.
3. User Agent (UA) is a process that assembles a collection of user identities and attributes to be transmitted to an RP in accordance with user or device owner intent.
4. Identity Provider (IdP) contains identities and attributes of users.
5. Relying Party (RP): A service provider that needs a collection of claims to provide that service. The claims may relate to financial responsibility or other user attributes that are required by regulation to meet legal responsibilities. It is beyond the scope of this use case to determine whether the RP actually has any justification in requesting any user attribute at all.
6. Registration Authority (RA) is a service that can register other actors; in this case the RA needs to attest to the trustworthiness of the UA.
7. Identity Ecosystem: a set of conventions for actors to exchange trusted claims. In this case the ecosystem needs to provide taxonomy of claims requests to be sent from the RP to the UA for user decisions on which attributes to share with the RP.

Goals / User Stories

1. Compliance with regulations for RPs and IdPs.
2. Common method for reliably describing and reporting an individual user's intent.
3. High comfort level for users that they have control over selectively shared information.

Assumptions

1. The RP has a relatively clear set of privacy compliance regulations to follow.
2. Standards will exist that permit the composition of claims by the UA in a format acceptable to the RP.
3. It is possible for an RA to reliably report to an RP that a UA is trusted to reliably convey user identities and attributes only in accordance with user intent. In the case of a

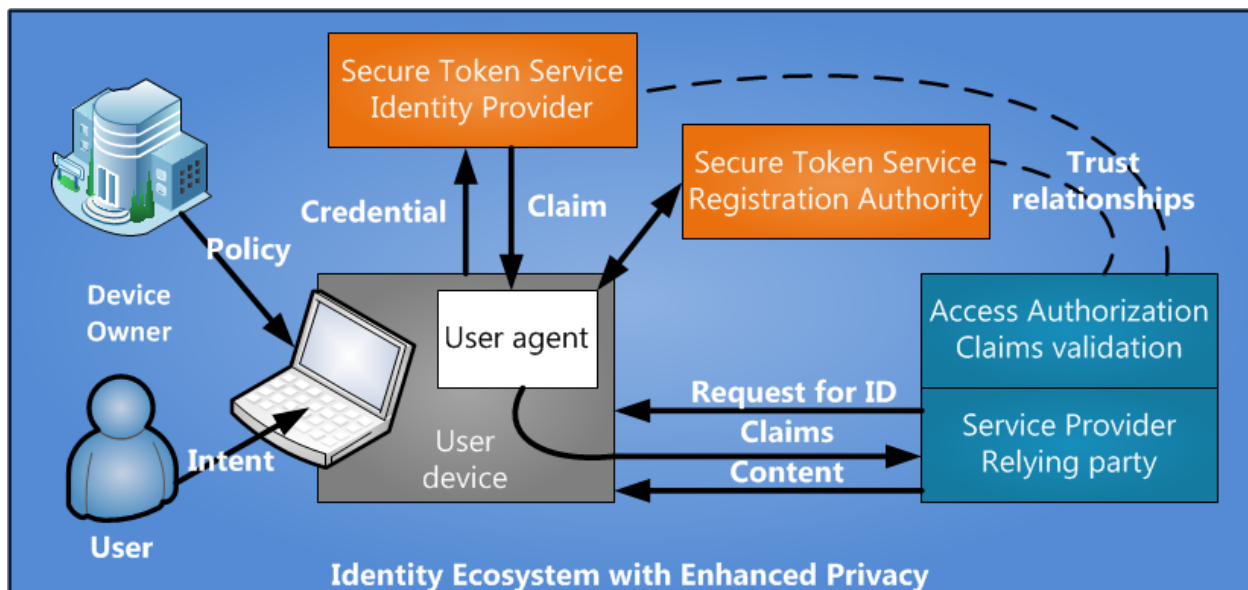
privacy enhanced technology provider in the cloud, the RP may be able to trust it directly.

4. Individual users have access to a digital device upon which they can depend to host a user agent that can represent their intent in a common digital format.
5. Registration Authorities exist and have a common protocol and taxonomy to report on UAs to RPs.
6. Public audibility of the open standards and code of UA systems in order to check the sharing of data and identity.

Process Flow

1. The user establishes an account with one or more IdPs. In this case there is no need to distinguish between identity providers and other attribute providers.
2. The user accesses a web site which requires identity attributes of some sort to continue to process the user request. The web site then becomes a relying party.
3. The RP uses a standard protocol and taxonomy to request the information needed from the user.
4. This request for information is intercepted by an agent for the user that can:
 - a. Determine if the information is available
 - b. Determine if the user has already authorized release to this RP
 - c. Display any remaining choices to the user to acquire more attributes or release those already available.
5. Format the set of requested claims into a response in a way the RP can evaluate the claims.
6. Send the response to the RP who has sole responsibility to determine if sufficient identity has been proved to provide the request access.
7. Repeat these steps until the RP is satisfied or one side gives up.

Note: This model works now for smart phones releasing user data to the internet because a small taxonomy of user information is reported. If the list grows long, the user experience is known to suffer as the display becomes too long for users to quickly scan before they assent. In no case should a user ever be asked for more types of information than can be displayed on a single screen with the acceptance button.



Success Scenario

1. Modern devices in common use for connecting users to the internet now come with a root of trust that can be used to report on the health of the device.
2. User agents are created on a user's device or in the cloud that can be audited to assure that they report only identity and attribute information the user wishes to release.
3. A small common taxonomy of user private data is established to enable RPs to request information, and to enable users to understand the information that has been requested.
4. The success metric should be that users are shown to be able to make intelligent choices given the displayed list of fields requested by the RA. Note that in some cases the data display to the user, e.g. date of birth will not be the same as the claim provided to the RP, e.g. over age 21. These cases are especially challenging for the user interface designer.
5. User choices are collected by the user agent so that if the same information has been requested by the same RP in the past, the user is not continually bothered with the same questions.

Error Conditions

1. User does not have the credentials required by the relying party. Mitigation: the relying party redirects the user to one or more sources of appropriate credentials.
2. The user agent loses the trust of the RA and hence of the RP. Mitigation: the user must be given actionable steps to get their agents back in compliance. It should never be the case that an "unauthorized" message be passed to the user with no remediation action indicated. Recall that for this case the user agent is under user control. In cases where

the privacy enhancing technology provider is in the cloud, the user is not part of the remediation process.

Relationships

1. An overall privacy use case showing the relationship between this use case and similar use cases can be found at:
https://www.idecosystem.org/wiki/Privacy_Enhancing_Technologies
2. The Device Integrity is defined the use case at
https://www.idecosystem.org/wiki/Device_Integrity_supporting_User_Authentication

References and Citations

1. COPPA is the Children's Online Privacy Protection Act that is well described in:
http://en.wikipedia.org/wiki/Children%27s_Online_Privacy_Protection_Act

NSTIC Guiding Principles Considerations

Privacy Considerations

Privacy enhancement is the core of the purpose of this use case. One particularly challenging problem is the case of minors under the age of 13 that are covered by COPPA. Those challenges are left for another use case.

In the following comments PII (personally identifiable information) is used in the broad sense of information that could allow linkage of an online identity to one specific carbon-based life form.

The following points address the concerns of the privacy committee as described on the discussion page:

1. Several actors get access to user's privacy information as a part of the regular business operations. Beside the general use of care as described in any identity ecosystem agreed between the parties the following comments might help in an implementation of this use case: 1a. The Registration Authority (RA) that attests to the trustworthiness of the user agent (UA) will receive information about a piece of code that could be linked to an individual user. That makes the identity of the user agent instance PII that needs the normal protection of PII. Implementers should consider implementations that do not require the RA to have knowledge of all possible relying parties. 1b. The Identity Provider (IdP) must have sufficient information to accept credentials from the user and authenticate that the user has the right to that particular identity. In a fully protected exchange the IdP should not be able to ascertain which other identity or attribute providers are accessed by the user or which RP is the source of the inquiry.

2. The user is given the option to select that the user agent (UA) will track their connections to relying parties to reduce the number of times that they are asked to approve release of the same information to the same party. The working assumption is that RPs are reliably identified and trusted to receive the user information. As a result the UA will contain a large amount of information about where the user navigates and what information they have provide to which RPs, not unlike the current situation with cookies on the user browser. Clearly the UA needs to be trustworthy of this burden. In addition, implementers should consider where the user agent is located and provide adequate controls to protect user privacy.
3. Claims persist on the UA in the same way that cookies persist on current UAs known as browsers. It is expected that by identifying the responsibility of the UA to the user it will be possible to create compliance criteria for UA that will allow them to be both useful to the user as well as respecting the user's wishes. It is recognized that this is a tough requirement that will require years to get right.
4. The RP can request any claim that they wish. As described in the usability section it is critical that the user be given sufficient information to evaluate the reason for the request within the stated constraint that all such UX must fit on a single page if we are to expect the user to tolerate the intrusion in their goal, which is to get access to the resources on the RP.

Security Considerations

In general security is not considered in this use case as security will be provided by the same type of credentials, token and claims as used in any secure implementation.

User Experience/Usability Considerations

One important part of any use case is the intelligibility of the choices presented to the user. Here it is very important that the user be give only some decisions to address as can easily and comprehensibly be display on the device that is used. In particular it is important that the RP have taxonomy of requested attributes or groups of attributes for presentation to the user within the scope of a single device page. That implies that the taxonomy of requested fields needs to be limited to those items that the user can sensibly be expected to comprehend.

Interoperability Considerations

This process is designed to interoperate with existing SAML, JWT and other token types. Token composition is not well defined in any extant standard and needs to be addressed by the ecosystem.

3.9 Trust Elevation Use Case

Use Case Description

Establish a user's identity with an unverified identity claim and raise the level of authentication using credentials with higher trust levels as needs dictate. The particular scenario described below is based on a user that has a low trust identity at some benefits provider that needs to be elevated in order to complete a sign up for benefits. This same flow should work in many other scenarios as well.

Actors

1. Financial institution - typically a federal depository institution (FDI).
2. Benefits providers - typically a governmental entity e.g. SNAP commonly known as the food stamp program fills the role of attribute verifier. The claims provided by a benefits provider have nearly the exact opposite meaning of claims in the case of a health insurance provider. In this case, the claim is an assertion of the availability of compensation to the RP for service provided to the user.
3. User - typically a human being acting through a user agent that needs to evaluate benefits of service providers.
4. Relying parties (RP) - a provider of services to the user.
5. Identity providers - typically a government sponsored provider, e.g. a state DMV or contractor.

Goals / User Stories

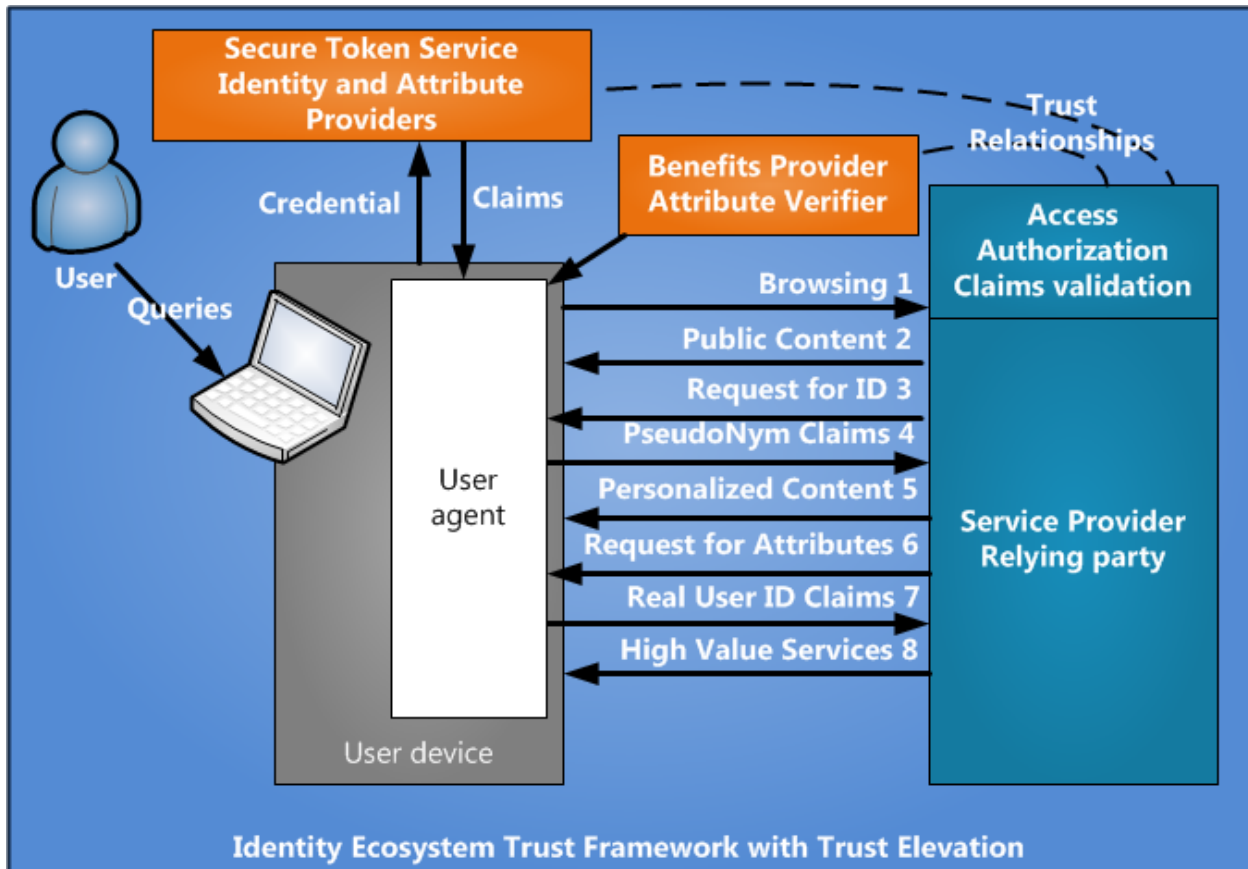
1. Low barriers for new users to evaluate relying party's services.
 - i. Note: It may not be required that the user go to higher levels of assurance unless the user desires access to specific services that require higher levels of assurance.
2. Fraud reduction which may imply cost reduction for the relying party.
3. Viable business model for the identity provider.

Assumptions

1. The relying party has a service to offer that the user needs to understand better before making a commitment to offer more of their own identity to the relying party.
2. The relying party requires an external proofing service to provide a higher level of assurance before full access to site may be granted.
3. User has a device with internet access.
4. Relying Party has a list of trusted Identity Providers.

Process Flow

1. The user accesses the relying party anonymously seeking information about the service offerings. (Flows 1 and 2 in the accompanying figure.)
2. The user wishes to establish a profile to create a continuing identity with the site.
 1. The site offers a selection of identity providers, perhaps including itself. (Flows 3 and 4)
 2. Each identity provider choice includes a link to acquire a credential.
3. The user goes to that identity provider and satisfies their need for high level authentication as required by the relying party. (Flows to the IdP)
4. The user device receives and stores the credential in the manner consistent with the level of assurance required by the relying party.
5. The user returns to the relying party and continues the access for services that are personalized for that identity. (Flow 5)
6. The user seeks to acquire high value services which cause the relying party to request claims that include the user's real ID from the user's device. (Flow 6)
7. A user agent on the user device determines if the user:
 1. Has the proof-of-presence needed for authentication, e.g. biometrics.
 2. Has protected the credential at the required level.
 3. Verifies the identity of the relying party.
 4. Has authorized the release of the information to the relying party.
8. The user agent sends a collection of claims as authorized by the user. These claims can come from the IdP as well as other providers as required by the relying party. (Flow 7)
9. The relying party either accepts the collection of tokens or requests more. Note that it is entirely the responsibility of the relying party to determine if the identity and attribute claims are sufficient to allow access. The user may have held back some claims for privacy reasons to prevent the relying party from granting access.
10. The user agent may respond with more information or not as authorized by the user and returns to step 6 or terminates. There is no guarantee that the user will have (or release) all of the claims needed by the relying party to grant access.
11. When the Relying party has received sufficient claims from the user the services are provided. (Flow 8)



Success Scenario

1. User can access the state benefits office to determine what benefits are offered and how they can qualify to receive them.
2. The benefits offices have access to a high assurance identity provider, such as the DMV.
3. The user goes to the DMV with the required documentation and gets the license delivered in the manner required by law. This may require multiple attempts.
4. The user is required to visit a benefits office in person one time to provide proof of presence. Deputy Registrars are enabled to provide this service in many state office buildings and approved notary publics in banks and other institutions.
5. A credential like a smart card is available to the user to acquire the authorized benefits.
6. The user is able to revalidate their access to the benefit as often as required to maintain timely access to the benefit.

Error Conditions

1. User does not have the credentials required by the relying party. Mitigation: the relying party redirections the user to one or more sources of appropriate credentials.
2. User cannot acquire the requisite credentials. Mitigation, the user needs to find the proof needed to satisfy one of the identity providers acceptable to the relying party.

- i. Note: In some scenarios the user may not be required to acquire another credential.

Privacy Considerations

Note that there is no reason for validation of attributes until the user decides to ask for specific resources (benefits in the present use case.) However it is known that search terms alone are sufficient in many cases to allow identification of the user. In any service that collects attributes or behaviors of the user, over time, only policy enforcement will offer any hope of blocking discovery of the user's identity. Implementers should consider implementations that do not allow parties to the transaction to correlate users with relying parties.

3.10 Four Party Authentication and Authorization Use Case

Use Case Description

NIST Interagency Report 7817 titled '*A Credential Reliability and Revocation Model for Federated Identities*,' provides a model to track the revocation status and overall reliability of credentials by having various participants report misuse or other risk factors to a service that can track the reliability of the credential. This report introduces a clear model of different ways for a service party or relying party to perform authentication and access control based on interactions with identity and attribute providers. The most robust example in the document is referred to as the Four Party model due to the number of actors involved in the process. It describes a case in which a Service Provider obtains information about a User sufficient to make an access control decision based on identity and attribute information gathered from the Identity Provider and Attribute Provider.

Attributes upon which access control decisions might be made may include age, location (residence address or current geo-location), biographical information including employment current or history (e.g. military or veteran status, access granted to employees of member companies, etc.), professional skills (e.g. medical or first responder status), law enforcement status, health plan membership, organization membership.

This use case does not incorporate the credential reliability and revocation features proposed in NISTIR 7817, but we recognize that revocation is an important topic.

Actors

1. Identity Provider - Establishes and manages users community digital identities. These identities in the form of digital credentials are employed by users to authenticate to service providers. The digital identity technology deployed by an Identity Provider for

the population of its users varies, and often dictates a specific authentication solution in order for the service provider to authenticate the user.

2. Attribute Provider - Vouches for attributes requested by the Relying Party. The need for attributes to user identification and authentication stems from access control models in which combinations of attributes (authorization attributes) are evaluated at the access decision point to the service to determine authorized access. This includes two models – single source and multi-source. In the single source model the service provider relies on a single source to provide attributes in an authentication event. In the multi-source model the Relying Party uses several independent attribute providers to provide attributes in an authentication and authorization event.
3. Relying Party - A Service Provider relies on identity and attribute information to make a decision to grant access to resources. In federations, service providers relinquish control of maintaining their own population of user credentials by accepting credentials managed by a third-party identity provider.
4. User - Individuals who wish to obtain access to Relying Party's resources.

Goals / User Stories

From the User's point of view, the goal of the use case is to obtain access to Relying Party's resource. From the Relying Party's point of view, the goal is to identify the User and obtain sufficient attributes to deny or grant access. From the Identity Provider's point of view, the goal is to issue credentials to Users and support the subsequent authentication of those credentials. From the Attribute Provider's point of view, the goal is to provide attribute information for uniquely identified individuals.

Assumptions

User has been identity proofed and obtained credentials from an Identity Provider that uniquely identifies the user. Depending on how this is implemented, the result may be a unique identifier or a collection of attributes sufficient to identify the user e.g. Clark Kent from Smallville. The user's unique identifiers may be verified by an Attribute Provider. If unique identifiers or a collection of attributes are linked to a user, the Relying Party may also verify unique identifiers or user attributes via Attribute Provider.

Process Flow

1. User accesses Relying Party to obtain access to resources
2. As necessary, the Relying Party communicates with User and Identity Provider to authenticate the User. This mechanism will be credential dependent.
3. Relying Party communicates with Attribute Provider to obtain attributes for the User based on the User's identifier obtained from the authentication.

4. Relying Party makes an access control decision based on the attribute information received.

Success Scenario

1. User authenticates successfully.
2. Attribute Provider delivers verified attributes to the Relying Party.
3. Relying Party makes an access decision based on the User's attributes.

Error Conditions

1. Attribute Provider cannot identify User based on identifier or identifying information provided by Identity Provider.
2. RP cannot communicate with AP or vice versa. AP provides inaccurate information. User provides inaccurate information to AP.
3. User provides inaccurate information to Identity Provider.

Relationships

1. Extended by:
 - Authenticate Person is a step in this process
 - Credential Issuance is a prior step in the process
 - Identity Proofing is a prior step during Credential Issuance

References and Citations

1. NISTIR 7817, *A Credential Reliability and Revocation Model for Federated Identities*

Privacy Considerations

1. Tracking policy determinations across different services a concern could provide substantial information about user behavior, and could be significantly identifying.
2. Depending on the variance in the types of actors, other considerations like user consent would be an issue.
3. Services can also lock out users with strict policies creating incentives for disclosure. One particularly challenging problem is the case of minors under the age of 13 that are covered by COPPA.
4. Attributes are potentially highly identifying, even without PII. Example: service member of specific age range, in a specific geographic area, could be enough to ID user. Will require work with RPs to ensure that collection of validated attributes is protected in order to be successful.

3.11 Unserved and Underserved People Use Case

Use Case Description

Unserved and Underserved refers to people who either do not have or have inadequate digital identities to enable them to participate in the secure and resilient, cost effective and easy to use, privacy enhancing and voluntary interoperable online Identity Ecosystem envisioned by NSTIC and the IDESG. Currently there are barriers to and opportunities for the Unserved and Underserved to enter the IDESG Identity Ecosystem. A few such barriers may be: limited financial means, physical disadvantage or challenge, language differences, and loss of employment. Such opportunities may be new products and services to remove these barriers, innovations in serving this community as well as greater social cohesion and internet-wide cyber-security.

Importantly, many of the Unserved and Underserved are also financially unserved and underserved. Today 68 million American adults are unbanked or under banked. More than 2.5 billion adults around the world are unbanked.

The goal of this use case is to leverage existing programs and services. In the US for example, the FDIC "Safe Account" program, to allow the Unserved and Underserved to use their "Safe Account" bank account enrollment process as a means of obtaining a digital identity and entering the IDESG Identity Ecosystem. Being Unserved and Underserved is not a new problem but one that has had a long and often intractable set of complexities perhaps going back to the beginnings of money and then banking. The efficiencies of cyberspace, i.e. the internet, provide an historic opportunity to bridge this gap.

Scenario (Example):

Julia, a prospective underserved financial services customer, wants to open a bank account as well as obtain a digital identity for use in the IDESG Identity Ecosystem.

Julia learns of a FDIC "Safe Account" type of account at her local community center which allows her to apply for an account and subsequently obtain a digital identity. Julia applies for and gets an FDIC "Safe Account" through an FDIC insured bank or equivalent financial institution compliant with 31 CFR 1020.220 - Customer identification programs (CIP) for banks, savings associations, credit unions, and certain non-Federally regulated banks or other acceptable customer identification program. The enrollment vetting process into a "Safe Account" serves the vetting requirements for Julia to obtain her digital identity. After a period of successful Safe Account practices Julia uses her Safe Account history and digital identity to apply for an FCCX credential or other governmental credential for accessing government services. Julia receives the government credential and uses the government credential to apply

for other online services and products including more financial services. Julia is able to step by step build access to a wide range of products and services she will need and use as she provides for her family and builds her entrepreneurial life as a clothes designer and pattern maker.

Goals Summary:

Julia will be able to obtain a digital credential with the qualifications used to obtain her Safe Account. Julia will be able manage her finances in a secure and insured or protected environment where she can increase her income through entrepreneurship, improving the quality of life for herself and her son, the economic activity in her neighborhood through her purchases, and tax receipts to her city and state. Julia will be able to interact with some government and non-profit services improving confidence in government and non-profit institutions and financial institutions including banking. The financial institutions and non-profit organizations, government agencies and healthcare providers will be able to increase the number of their customers/participants. Through this use case a broad range of stakeholders are brought together to share risks and rewards in creating an online Identity Ecosystem Framework where economic opportunity, productivity and human well-being are harmonized.

Actors

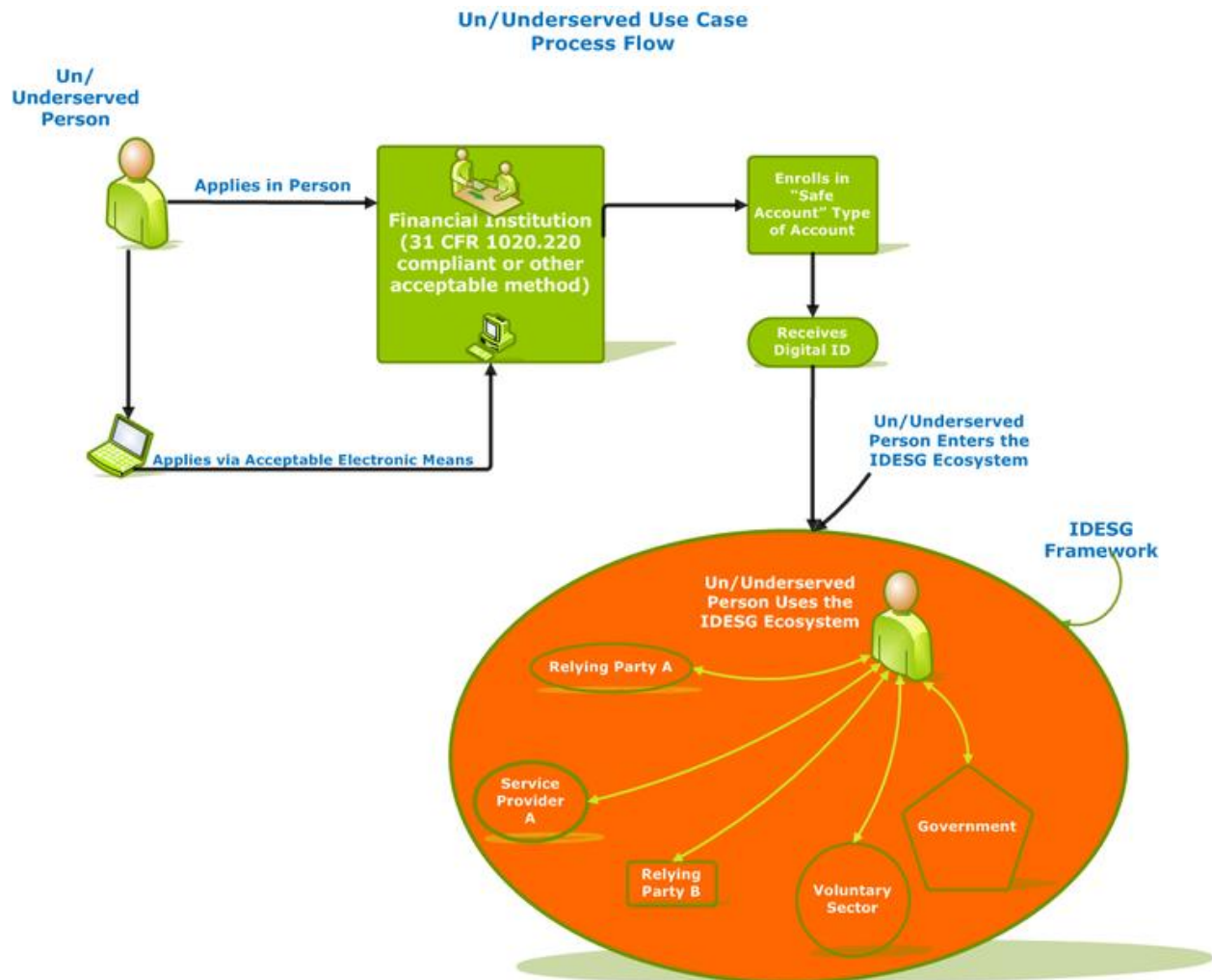
1. Unserved and Underserved People
2. Financial Institutions
3. Non-profit Organizations
4. Government
5. Any Relying Party or Service Provider in the IDESG Identity Ecosystem that complies with the NSTIC principles and has a Trustmark Accreditation.
6. Alternative Financial Services.

Assumptions

1. Unserved and Underserved Person applies in person at the Financial Institution or uses an acceptable electronic means of application including for example Treasury's OCIP that has brought together the FSSCC, DHS, and NIST to create a Cooperative Research and Development Agreement on identity proofing, which has identified new methods for satisfying the "know your customer" requirements of financial institutions.
2. Financial Institution must be a FDIC insured bank or equivalent. The digital identity meets the needs of relying parties.

Process Flow

1. This use case is unique in that the person, Julia and her son in this case, exist outside an online Identity Ecosystem. Entering the Identity Ecosystem is a kind of state change for Julia. The other stakeholders are already inside the Identity Ecosystem.
2. The process of entering the ecosystem should be done with care by all stakeholders.



Success Scenario

Julia is able to enroll in a Safe Account that provides her with a digital identity useful in the ID Ecosystem for products and services and for federal, state and local governments. Julia can also apply for and potentially receive other digital identities from other ID Ecosystem providers enlarging the range of products and services, including financial she can access.

References and Citations

1. ("Safe Accounts are checkless, card-based electronic accounts that allow withdrawals only through automated teller machines, point-of-sale terminals, automated clearinghouse pre-authorizations, and other automated means and which has lower-cost, electronic payments and prohibits overdraft or non-sufficient funds fees.")
2. Consumer Privacy Bill of Rights
3. Fair Information Practice Principles (FIPPS)
4. FDIC Model Safe Account Pilot (<http://www.fdic.gov/consumers/template/>)
5. Federal Cloud Credential Exchange (FCCX)
6. According to the 2011 FDIC National Survey of Unbanked and under banked Households, September 2012, 68 million American Adults, making up 30 million American Households, are either unbanked or under banked. Safe Account Final Report (<http://www.fdic.gov/consumers/template/SafeAccountsFinalReport.pdf>)
7. Federal Identity, Credential, and Access Management (FICAM)

3.12 Selectively Disclose Attributes Use Case

Use Case Content

A Claimant possesses multiple attributes and is eligible for different benefits and/or online services from a Relying Party based on specific attributes. The attributes addressed in this use case can include identity attributes (i.e., name, address, phone number) and biographical attributes (i.e., age, individual certifications, professional affiliations). The Relying Party offers a benefit or service if the claimant discloses the attribute in order to prove eligibility for the specific program. In this use case, the Relying Party is only interested in the specific attribute information and the claimant needs a way to disclose that attribute information.

Actors

1. Claimant: a human individual who wants to demonstrate some claim of an attribute.
2. Relying Party: an organization wanting to deliver a benefit or service to individuals.
3. Attribute Verifier
4. Registration Authority

Goals / User Stories

John realizes that he is eligible for a benefit from an organization that offers an exclusive benefit/service for people who possess the same attribute as John. The organization wants to verify that John is actually eligible for



the benefit/service to protect themselves from fraud or abuse. John is able to provide the minimum necessary information to a third-party attribute verifier who then matches that information against an authoritative source. John is able to review the information before it is shared back to the organization offering the benefit. If John authorizes the release of the information, the organization unlocks the benefit/service to John based on a "yes" or "no" response. The goal of this use case is to protect John's privacy while giving him access to the benefit and at the same time protecting the organization from fraud and abuse. The organization is also able to grow their market share with the community of people possessing specific attributes.

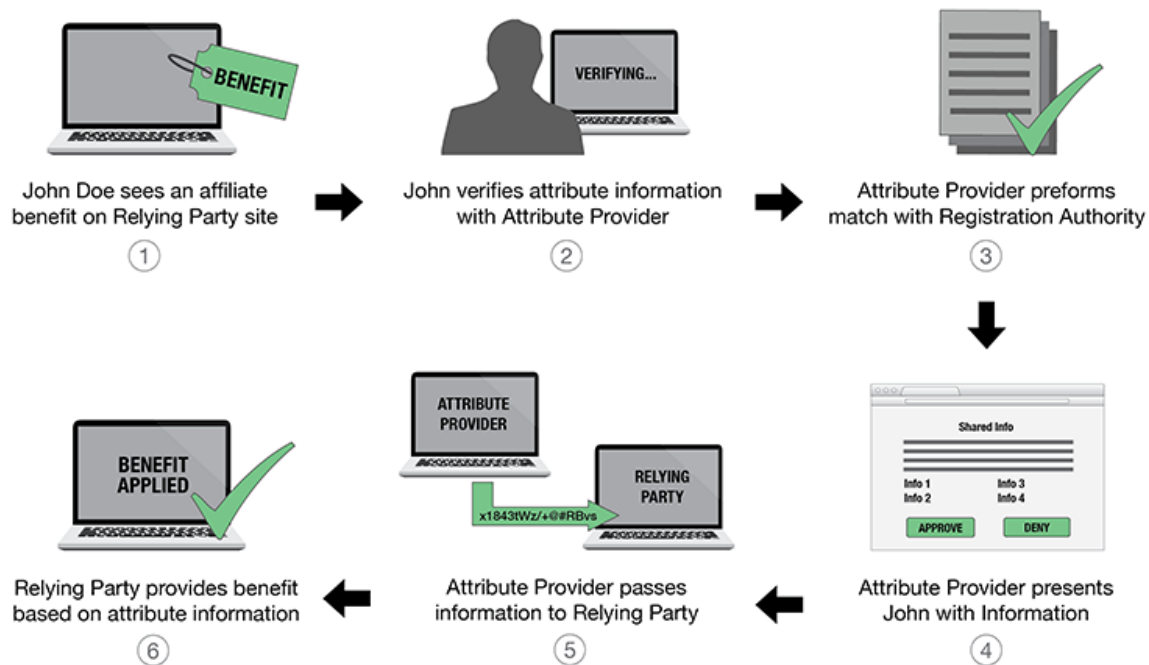
Assumptions

1. Relying Party only requires the attribute information be verified and not the identity of the claimant.
2. The Relying Party does not need to uniquely identify a single person.
3. Relying Party requires the attribute information to be verified against an authoritative source.
4. An authoritative source exists to proof the attribute assertion of a claimant.
5. Attribute Verifier is able to verify the attribute information of a claimant against the authoritative source.
6. Relying Party has an existing relationship with an Attribute Verifier that provides an acceptable level of assurance based on the value and risk of the benefit or service.
7. Attribute is bound in some way to limit its scope. That can include (but is not limited to) a pseudonym, timestamp, session ID or other item that will prevent a replay of the attribute claim.

Process Flow

1. A Claimant sees they are eligible for a benefit or service on a Relying Party site based on an attribute the user possesses.
2. The Claimant chooses to prove to the Relying Party that he possesses the attribute and qualifies for the benefit or service.
3. The claimant verifies attribute information with an acceptable Attribute Verifier.
4. The Attribute Verifier performs a match with the authoritative database associated with the particular attribute.
5. The Attribute Verifier presents the results of the match against the authoritative database and gives the user control of whether or not that information is shared with the Relying Party.

6. Upon authorization by the Claimant, the Attribute Verifier passes the minimum attribute information to the relying party to prove the Claimant is eligible.
7. The Relying Party unlocks the benefit or service for the Claimant upon receiving confirmation from the Attribute Verifier that the user is qualified.



Success Scenario

1. The Claimant is able to access a benefit or service online by proving that they possess a specific attribute.
2. The Claimant is then able to disclose their attribute information without having to re-verify.
3. A Relying Party realizes a reduction in risk through the use of verified attributes.
4. A Relying Party is able to grow market share and loyalty with people possessing specific attributes.

Error Conditions

1. The Claimant possesses the attribute, but is not able to verify that attribute with the Attribute Verifier.
2. The Claimant does not possess the attribute, but is able to verify through the Attribute Verifier and fraudulently access the benefit or service.
3. Someone other than the claimant is able to present the attribute token in a replay outside of the authorized scope and gain access to the benefit or service.

References and Citations

1. FTC Fair Information Practice Principles
<http://www.ftc.gov/reports/privacy3/fairinfo.shtm>
2. NSTIC Strategy,
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
3. NIST SP 800-63-2
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

Privacy Considerations

1. Claimant should be able to voluntarily participate in the process.
2. Claimant should control the rights to their own data and that Claimant's information should only be released to a Relying Party at the claimant's discretion.
3. Organizations shall limit the collection and transmission of information to the minimum necessary to fulfil the transaction's purpose and related legal requirements.
4. Same concerns about the identifying properties of validated attributes as above use cases.
5. Attribute provider appears to pass info directly to the relying party, enabling it to track the claimant's interactions with the relying party.

3.13 Remote Electronic Identity Proofing Use Case

Use Case Description

The core function of this Use Case is to streamline the identity proofing process engaging live human interaction virtually via video conferencing. Additionally, this Use Case is fundamentally different and considers between physical face to face in-person identity proofing in contrast to a real-time virtual face to face in person identity proofing meeting using video conferencing that is recorded, to capture claimants/subscribers verbal and written statements, identification document images, oath based under penalty of perjury, attributes, and facial/voice biometrics.

Actors

1. Identity Manager collects a set of attributes for identity verification - (IM)
2. Claimant/Subscriber - (C)
3. Public Claimant/Subscriber - (PC)
4. Registration Authority/Credential Service Provider - (RA/CSP)

Goals

1. Claimant, who is distal (not in the physical presence) of RA and has an antecedent relationship with the RA, is given approval by RA to acquire a trusted credential.
2. Public Claimant is remote (not in the physical presence), **does not** have an antecedent relationship with an RA and requires a trust credential.

Assumptions

1. Claimant/PC needing to initiate the process for acquiring a trust credential is in the physical presence of the Identity Manager to present their attributes.
2. RA/CSP has a pre-authorized trust relationship with IPVSP.
3. RA/CSP has issued to the Identity Manager (IM) a method for the collection of the required Claimant/PC attributes.
4. Identity Manager (IM) must have a trust relationship with RA/CSP.
5. Claimant/PC is distal or remote (not in the physical presence) of the Identity Manager System and device used in method for attribute collection, attestation, and digital signing.
6. IP and Claimant/PC process the collection of attributes via prescribed method to include accordance with 28 U.S.C. 1746 (declaration under penalty of perjury) and provisions in FBCA 3.2.3.1 authentication of Human Subscribers.

Process Flow

1. Claimant/PC initiates remote electronic identity proofing event via on-line appointment. If PC, payment for services options are necessary.
2. Identity Manager retrieves request. Identity Manager confirms payment receipt if service is for PC; however Identity Manager implements attribute collection methodology via video conferencing.
 - It is contemplated that attribute collection methodology via video conference may interface with CSP platform to streamline trust credential enrollment processing and issuance.
 - It is also contemplated to augment high assurance identity proofing to include collection of biometric attributes in accordance with FIPS 201-1.

Success Scenario

1. Claimant/PC who is remote (not in the physical presence) of the RA/CSP securely submits their attributes to Identity Manager maintaining IDESG privacy standards.
2. Identity Manager submits Claimant/ PC's attributes to RA/CSP for authentication, and digital identity trust credential is issued to Claimant/PC.

Error Conditions

1. Claimant/PC submits fraudulent attributes.
2. Claimant/PC does not have required identification documents.
3. PC fails to make payment.
4. Claimant/PC attributes do not comply with RA/CSP authentication standards.
5. Communication transmission between Claimant/PC, IM, RA/CSP, disruptions.
6. Claimant/PC or Identity Manager does not have system or devices for implementation of attribute collection methodology.
7. Claimant/PC and/or Identity Manager inputs errors or create omissions in attribute collection.
8. Identity Manager does not have trusted relationship with RA/CSP.

References and Citations

1. NIST 800-63-1
2. Federal Bridge Certificate Authority
3. ISO/IEC WD1 29003 -- Information technology – Security techniques – Identity Proofing
4. FPKIPA – CPWG Antecedent, In-Person Task Group
5. FIPS 201-1
6. FIPPS
7. CPBR
8. VPPA
9. Privacy and Security Tiger Team Trusted Identity of Patients in Cyberspace
Recommendations on Patient Identity Proofing and AuthN
10. Patent Nos. 7590852, 8190904

NSTIC Guiding Principles Considerations

Privacy Considerations

It is expected that attributes gathered during identity proofing are sensitive information and deserving of privacy protections. In addition the Remote Electronic Identity Proofing Use Case recommends all actors refer to Fair Information Privacy Practice Principles (FIPPS), Consumer Privacy Bill of Rights (CPBR), Video Privacy Protection Act (VPPA, and the IDESG PEM for ongoing guidance as this Use Case is further developed and is not implementation specific. This Use Case presents possible privacy risk issues of Breach of Trust, Stigmatization, and Surveillance. These terms of risk are based on definitions from the “Taxonomy of Privacy” by Daniel Solove. Other than non-participation, to date there are no absolute solutions to prevent a breach of confidentiality. There are a variety of remedies that can be combined to offer an applicant relief from harm as well as support deterring breach of trust events.

Breach of Trust – Is cited as a breach of implicit or explicit trusted relationship, including a breach of a confidential relationship. The Federal Bridge Certificate Authority provision for PIV issuance states that a trust relationship between the Trusted Agent and the applicant can be based on an in-person antecedent identity proofing event and may suffice as meeting the in-person identity proofing requirement. Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the “FBCA Supplementary Antecedent, In-Person Definition” document. The FBCA document cites an Antecedent event is an in-person identity proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements. The fundamental remote electronic identity capturing functions of this Use Case are video conference and electronic signatures/records wherein the remote electronic identity proofing event is recorded with the consent of the applicant attesting to the genuine validity of their personal identifiable information under penalty of perjury. Additionally the Trusted Agent performing the identity proofing event should have an established trust relationship with a RA or CSP. Breach of Trust may be deterred due to the video recorded tracking of the participants being the applicant and trusted identity proofer. Remote electronic identity capturing functions, Opt out, tort of Breach of Confidentiality, Court Order Warrants, attestation under penalty of perjury, established trust relationships, and disclosure of using an applicants’ PII beyond its intended purpose are all components which may be combined to provide an applicant relief from harm and be leveraged as a deterrent in mitigating breach of trust.

Stigmatization – Is cited as personal data is linked to an actual identity in such a way as to create a stigma. This Use Case illustrates a new viable and standardized methodology for remote electronic identity proofing. However inherent in any identity proofing event is the goal of attribute collection for the purpose of establishing identity. The way attributes are connected to a person is not the purpose and function of this Use Case. This Use Case is solely and fundamentally purposed for the collection of the attributes to subsequently establish identity and credential issuance by a CSP. Connection of attributes is inherent in their collection via identity proofing, however this Use Case is not purposed to connect the attributes to establish identity. Out of scope attribute collection activity such as selling attributes for profit, generalized profiling, exploitation, and other unauthorized activity that use a set of attributes in a negative and often unfair manner is prohibited and such activity is subject to regulatory penalties provisioned for applicants harmed by such activity.

Surveillance – Is cited as the collection or use, including tracking or monitoring of personal data that can create a chilling effect on behavior including free speech and/or freedom of association.

The VPPA cites in Section § 2703

(a) Required disclosure of customer communications or records:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service:

A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection.

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) With prior notice from the governmental entity to the subscriber or customer if the governmental entity-

(i) Uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) Obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

Annex A – Acknowledgments

The UCAHG would like to thank Bryan Russell, Ann Racuya-Robbins, J. Andrew Hatter, Jim Fenton, Tom Jones, Bob Pinheiro, Scott Shorter, Matt Thompson, the Nym Issues Group, and Cathy Tilton for their participation and contribution.

In addition, appreciation is given to the members of the IDESG Standards Coordination Committee and other IDESG committees who contributed to and reviewed this document.

Annex B – References

1. National Strategy for Trusted Identities in Cyberspace (NSTIC):
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
(Source for NSTIC Guiding Principles)
2. IDESG Use Case Wiki: https://www.idecosystem.org/wiki/Use_Cases
3. OASIS Identity in the Cloud Use Cases: <http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html>
4. “Writing Effective Use Cases”, by Alistair Cockburn copyright 2001,
<http://www.infor.uva.es/~mlaguna/is1/materiales/BookDraft1.pdf>

Annex C – 2013 Goals

In May of 2013, the IDESG Plenary Chair, Bob Blakely, identified a set of goals to be achieved with the IDESG Use Cases. The following table discusses activity against these goals.

Goal	Explanation
Frame the IDESG's initial objectives and scope of work	The use cases contributed by IDESG members (over 50 from individuals, 20 from the UCAHG) reflected the interests and priorities of the contributors, and considerable discussion and effort has been put into obtaining the opinions of diverse constituencies within IDESG.
Drive consensus among IDESG plenary members about the characteristics of the ecosystem and identity ecosystem framework we are trying to bring into existence	This deliverable sketches a map with a few prominent landmarks. We call upon IDESG work groups to draw roads and settlements and fill in that map. Then the IDESG can discuss where to drive consensus to.
Capture the requirements of all NSTIC constituencies	Many constituencies did participate and the review process was open to all.
Make the application of the NSTIC principles to real-world scenarios concrete	Some are concrete, many are more abstract. The abstract use cases are molds into which the IDESG committees may pour concrete.
Serve as a test target against which developing IDESG work products can be evaluated	<p>Please submit these into evaluation methodologies, we welcome comments regarding:</p> <ul style="list-style-type: none"> • Security considerations (including assumptions, requirements, security levels, security policies, security evaluation techniques, etc.) • Privacy considerations • Relevant legislation, regulation, standards and/or best practices • Real world examples, NSTIC Pilots particularly welcome! <p>If the use cases selected for this publication are not the ones you would pick there are many more to choose from, and the process to contribute a use case is open to all IDESG members.</p>
Drive the development of evaluation guidelines which can facilitate granting of an IDESG Trustmark	These use cases are trial input to those evaluation guidelines. Consider them test grist for a prototype mill.
Provide a yardstick for measuring success of NSTIC pilot projects	This was outside our scope of effort. NSTIC pilot evaluation is not the mission of the use case UCAHG or the Standards Committee.