Use Case: Over 21 with Proof of Presence Token

Purpose:
To provide reasonably high assurance that a claim of majority is valid for acquiring restricted resources.

Goal:
To allow online purchases of legally restricted resources like alcoholic beverages in an environment where user identity attributes are distributed among many providers.

Actor: Consumer of restricted resources.
Actor: Supplier of restricted resources.
Actor: Verifier of claim of majority (also can validate binding to subject)
Actor: Provider(s) of late binding tokens and client-side code

Preconditions:

1. The Consumer has acquired a late binding token from any provider at all.
2. The Consumer has registered an over-21 claim with verifier using token.
3. The Consumer has established an account with supplier using a DID or other persistent ID.

Scenario: Consumer signs into supplier and has never purchased liquor from this site.

1. Consumer selects to purchase liquor item
2. Supplier asks user for over 21 proof with a nonce.
3. Consumer sends verifiable claim of over 21 they acquired from verifier.
4. Supplier asks verifier for proof. (This would be by redirect to verifier through user browser)
5. Verifier supplies validated claim (or statement of non-revocation) bound to nonce by redirect to Supplier, if this VC is bound to the user's session with supplier, it can have a lifetime of the duration of bound session.
6. Monetization is by direct micro payment (on the order of $.05) from supplier to verifier.

Alternative Paths:

1. Consumer selects to purchase liquor item.
2. Supplier asks user for over 21 proof with a nonce.
3. Consumer asks verifier directly for proof with nonce from Supplier.

4. Verifier asks consumer to enter token for proof of presence.
5. Verifier send validated claim with nonce of supplier with short expiration time (10-20 mins - alternate life time of duration of session).
6. Consumer sends verified claim to supplier.
7. Monetization is by advertising from verifier to consumer.

A different path using biometrics:

Yoti, a London-based startup which wants to become the “world’s trusted identity platform”, is one of many attempts to provide such a service. Its system stores government id documents and biometrics. If a user wants to buy a bottle of wine at a supermarket self-check-out and needs to prove their age, they scan a qr code and take a selfie using Yoti’s app. The retailer can be sure of their age, but no one has seen their name or nationality. From the Financial Times.

Failed Paths:

1. User does not get verified claim for some reason.
2. Verified claims fails validation at supplier.

Accepted Risks:

1. The consumer is not over-21 and has buddy’s token to enter into computer.
2. Session hijacking mitigated with HTTPS and session cookies.
3. MitM attacks mitigated by hardware token bound to origin URL of verifier.
4. Note that the late binding token could be bound to supplier as well as needed.
5. The identity of the verifier/validator is discoverable by the supplier.
6. User makes choices on which attributes are trusted for sharing with the supplier.

Post Condition:

1. If validation accepted, and consumer completes payment, the restricted goods are shipped to the consumer by the supplier.
2. Note that at the end of the process of validating the user’s age, the state issued license to sell alcoholic beverages will determine which path to use. The penalty for the supplier using the wrong path is loss of the license to sell alcohol.

Examples:

1. Late binding token - FIDO U2F token, TEE TPM VSC, etc.
2. Client side code - javascript in a browser, native app, etc.

Dependencies::

1. Web Sites must be trusted before any user information is released.
2. Trust federations can be used to help users make informed decisions.
3. User consent and trust must begin with no user information transferred.
4. Standards exist to collect needed attributes where-ever they may be.

Workflow Diagram:
TK