Antoine Mason CIPP
amason@documentorchards.com

The Identity Management System must be free to consumers.

There should be at least three and no more than six Certificate Authorities (CA) who's only line of business would be the issuance and management of PKI certificates and tokens.

The token should not be branded, but would be similar in appearance and function.

A data subject enrollment should be a three part process:

1. registration -collection of biographical info

2. authentication -binding of attributes to a PKI based token

3. delivery - in-person delivery of the token and/or in- person activation.

All CA should be allowed to access a data subject's enrollment event to avoid duplication.

The PKI based token should attest to only the following attributes: Majority; Gender, at birth; and Allegiance.

Initially, there should not be a focus to capture biometrics, but to allow systems to mature.

The attributes to bind are:

-Majority: over age 18 -no reference to DOB or YOB

-Gender at Birth: male or female

-Allegiance-what economic community does the data subject pledges, ex: Western Hemisphere Free Trade Zone; European Economic Community; Aisan-Pacific Economic Cooperation; Asian Economic Community; African Economic Community, etc

The token would require a locational tracking capability. However, this capability must be machine read-only and should only be discovered for "break the glass" cases to resolves disputes, such as a Relying Party's claim of a purchase in Eastern Europe by Data Subject who was enrolled in North America and pledged to WHFTZ, and then only by the express written consent of the Data Subject or by law enforcement.

Authenticators- are not to be widely published, they are:

Something you know- password, unique account number or SSN

Something you have- ATM card, Real ID, Smart Card, Smart Phone, PKI-hard/soft tokens

Something you are- biometric, gender, age, behavioral characteristics.

Something in your time and place- IP address, GPS, Cloud Computing, RFID, linkable data, cookies

Something you pledge- socioeconomic and political affiliation, religious or philosophical beliefs, trade/union membership, National Allegiance.

Something that asserts you- Trusted third party, Registration Authorities andCredential Authorities ex-DHS Registered Travelers program.

Possession of a token should be considered to large extent as proof of who you are.

CA and the entities involved in the enrollment can make money every time Relying Parties ping the digital signature of the data subject. The cost to the relying party (RP) should be fractions of a penny.

PS: Note: A Data Subject will likely have to be enrolled twice, at age of 13 and 18.

--
Document Orchards LLC
"Protecting Your Visibility in a Transparent World"
IdM Enrollment
484/619- 3628