

UNPACKING AGE ASSURANCE: TECHNOLOGIES AND TRADEOFFS

Age Assurance is the umbrella term for existing and emerging methods used to establish an individual's age or age range. In a rapidly evolving regulatory landscape, there is no 'one-size-fits-all' solution; instead, policymakers and organizations should focus on proportionate, risk-based solutions tailored to specific use cases. By adopting a layered approach and leveraging emerging standards like ISO/IEC 27566, platforms can ensure that age checks prioritize functionality, performance, privacy, security, and acceptability.

AGE ASSURANCE QUESTIONS

WHAT ARE THE GOALS?

- Place an individual within an age threshold or age band. (e.g. 13-15)
- Limit access to an age-restricted service, provide age-appropriate experience or facilitate parental consent.

WHAT IS THE APPROPRIATE ASSURANCE METHOD?

Choose a method or methods that provides a level of age assurance (accuracy) proportional to the goals and risks of the service, keeping in mind that legal obligations may dictate a specific method.



DOES THE AGE ASSURANCE METHOD....

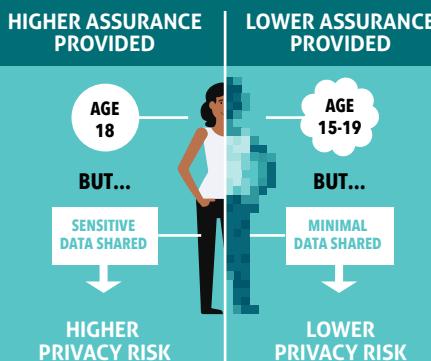
- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.



DECLARATION

A user self-asserts their birthdate without providing supporting evidence.

AGE-GATING

This common method is most appropriate in low risk situations, as children and teens can bypass by providing a false birthdate. Privacy risk is low, especially if birthdates are not retained or matched with a name or other indirect identifier.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

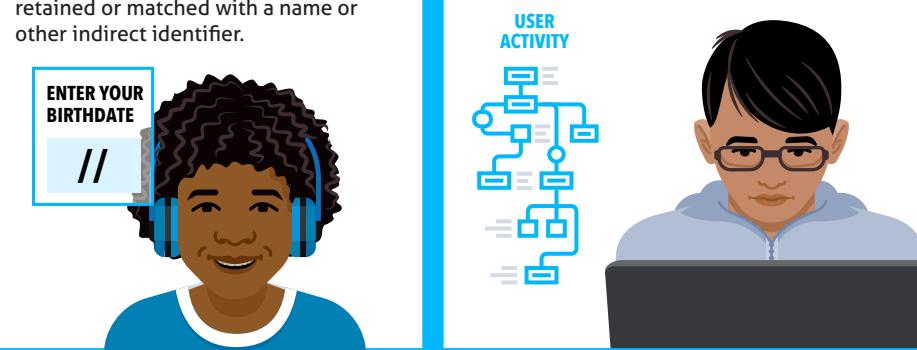
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

INFERENCE

Drawing reasonable conclusions about an age range based on user activity, financial transactions, email address, existing accounts, etc..

BEHAVIORAL / ACCOUNT

Email linked to workplace apps, mortgage lender, 401k provider. Login patterns show weekday activity during business hours. Usage profile—professional services, financial products—infers adult user.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

EXAMPLE USE CASE

AGE ASSURANCE FOR ONLINE GAMING

In this scenario, Miles, a 16 year old, is accessing an online gaming service that is designed for teens and older. It has optional age-restricted features.

INITIAL EXPERIENCE

DECLARATION

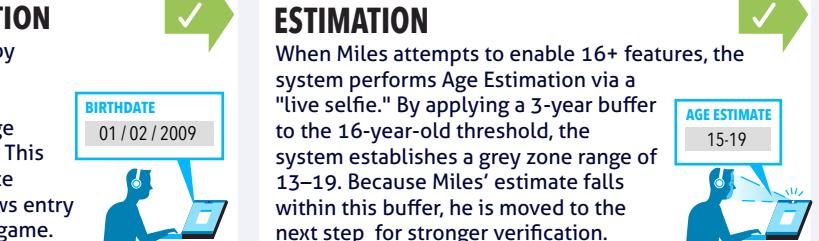
Miles starts by providing a self-asserted birthdate (Age Declaration). This low-assurance method allows entry to the main game.



SECONDARY FEATURE

ESTIMATION

When Miles attempts to enable 16+ features, the system performs Age Estimation via a "live selfie." By applying a 3-year buffer to the 16-year-old threshold, the system establishes a grey zone range of 13-19. Because Miles' estimate falls within this buffer, he is moved to the next step for stronger verification.



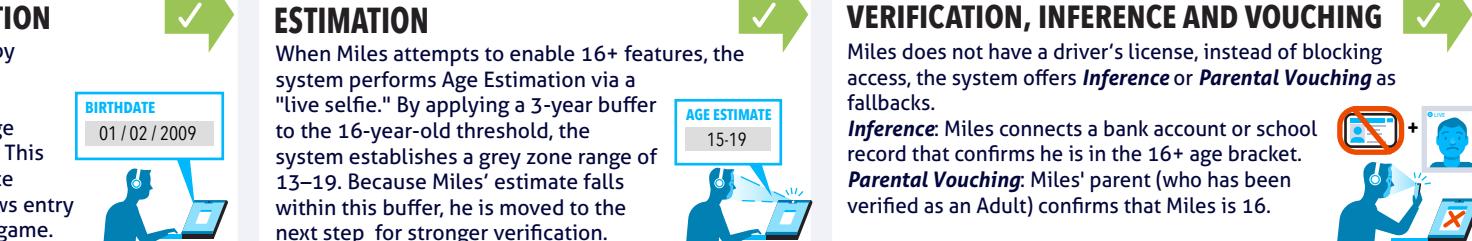
GREATER ASSURANCE NEEDED

VERIFICATION, INFERENCE AND VOUCHING

Miles does not have a driver's license, instead of blocking access, the system offers **Inference** or **Parental Vouching** as fallbacks.

Inference: Miles connects a bank account or school record that confirms he is in the 16+ age bracket.

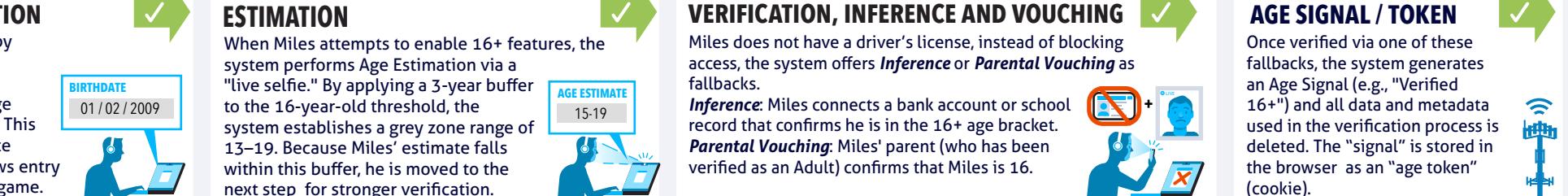
Parental Vouching: Miles' parent (who has been verified as an Adult) confirms that Miles is 16.



AGE SIGNAL / TOKEN

BINDING

Once verified via one of these fallbacks, the system generates an Age Signal (e.g., "Verified 16+") and all data and metadata used in the verification process is deleted. The "signal" is stored in the browser as an "age token" (cookie).

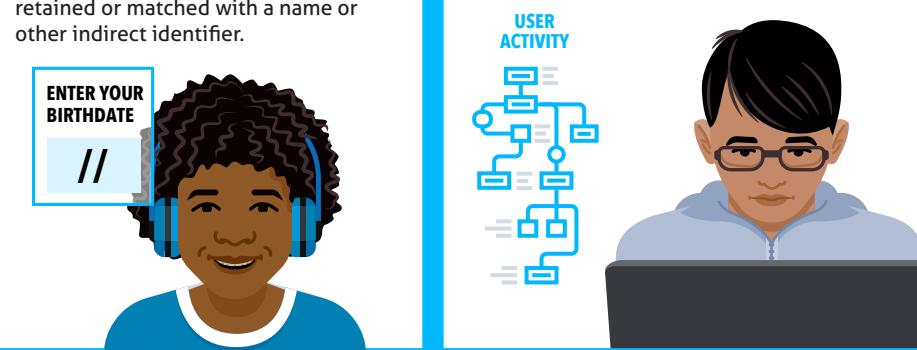


DECLARATION

A user self-asserts their birthdate without providing supporting evidence.

AGE-GATING

This common method is most appropriate in low risk situations, as children and teens can bypass by providing a false birthdate. Privacy risk is low, especially if birthdates are not retained or matched with a name or other indirect identifier.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

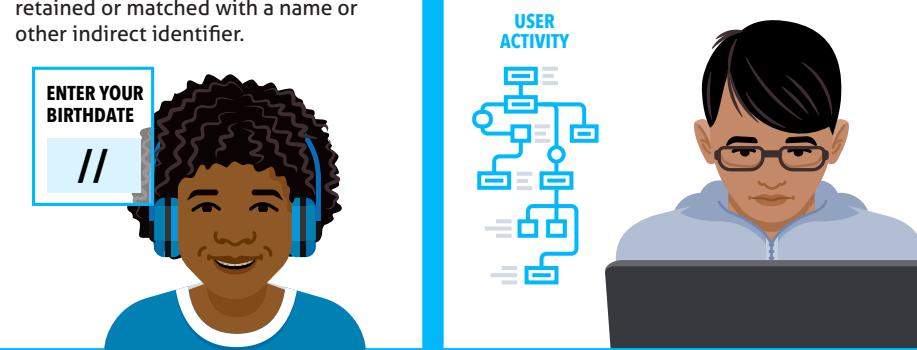
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

INFERENCE

Drawing reasonable conclusions about an age range based on user activity, financial transactions, email address, existing accounts, etc..

BEHAVIORAL / ACCOUNT

Email linked to workplace apps, mortgage lender, 401k provider. Login patterns show weekday activity during business hours. Usage profile—professional services, financial products—infers adult user.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

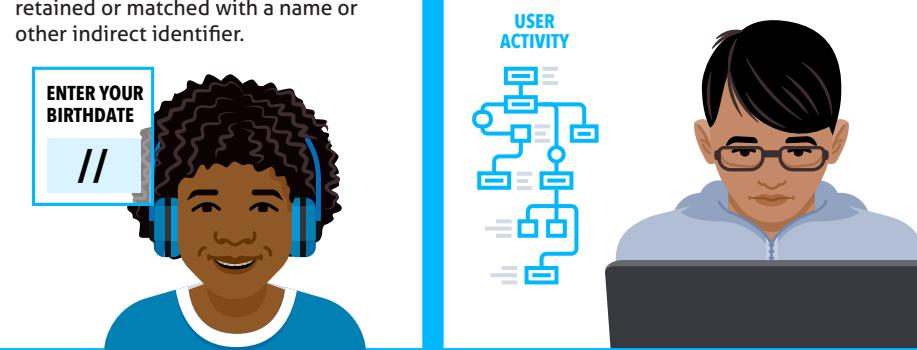
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

ESTIMATION

Using AI and machine learning to deduce likely age based on biological or behavioral traits e.g. face, voice, iris, typing patterns.

TRAIT CHARACTERIZATION

Estimates age using a facial image, but the individual is not uniquely identified. Best used to place users in age bands, or signal that a user meets an age threshold, such as under 13 or 21+. Estimation is less effective for discerning age in a narrow range like 17 vs 18.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

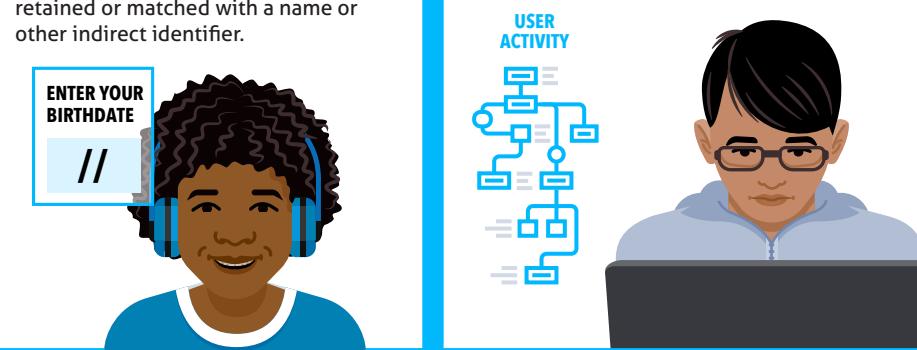
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

VERIFICATION

Determining age by referencing an authoritative, verified date of birth (DOB) from documents or databases.

ID + BIOMETRIC

Matches a scan of a government-issued ID and live photo or video using facial recognition. This method is more appropriate for regulated or higher risk age restricted services.



DOES THE AGE ASSURANCE METHOD....

- Provide a result that relates to the individual.
- Maintain low errors over different demographics.
- Facilitate access based on true positive (TP) and prohibit for true negative (TN) results.

WHO IS RESPONSIBLE FOR AGE ASSURANCE?

Answering this question requires policy and technical choices in a complex and evolving environment where age assurance functions may be split across the technology stack.

IS ASSURANCE BALANCED WITH PRIVACY RISKS?

After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

RISKS AND CHALLENGES OF AGE ASSURANCE

LIMITING ACCESS



LOSS OF ANONYMITY



SECONDARY DATA USE

