Age-Based Access Restrictions considerations

Authors: Gianpaolo Angelo Scalone, Kevin Smith

Affiliation: Vodafone

Submission preference: Public with attribution

1. Introduction

As digital content becomes increasingly accessible, protecting minors from harmful or inappropriate material is a growing concern for regulators, platforms, and infrastructure providers.

Age-based access restrictions are emerging as a key tool to address this challenge. Telecommunications providers ('telcos') offer unique capabilities for identity verification, persistent identifiers, and network-level enforcement.

This paper explores the technical and architectural implications of implementing age-based restrictions, with a particular focus on telco infrastructure. It also considers alternative verification methods, blocking mechanisms, and the governance of content restriction lists.

2. Regulatory oversight

Telecommunications providers are regulated in each country they operate by an NRA (National Regulatory Authority). This enforces obligations on each provider as a Data Controller (EU GDPR, UK) and adherence to Codes of Practice in relation to age-restricted content (for example, an age-verified opt-in to remove safe search flags).

3. Age Verification Methods

Telcos routinely collect and verify identity documents during mobile contract activation, especially in Europe, where most countries require ID verification for both postpaid and prepaid SIMs. For postpaid (pay monthly) subscriptions, a full credit check is typically carried out which will utilize tools from financial services regulated credit agencies which provide additional identity and age checks beyond physical credentials (driving license, passport, national Identity cards).

By default, SIM users are considered to be non-adult unless proven otherwise.

3.1 SIM-Based Verification (Telco-Centric)

The in-person document verification and additional credit agency check makes SIM-based verification a strong candidate for age assertion.

challenges	**mitigations**
Parents purchasing SIMs for children	User assertion protocols during activation
Corporate or shared accounts	Linked accounts for parent-child relationships
SIM swapping and device changes	SIM-device binding and re-authentication triggers 'opt-in' approach to unlock adult status

3.2 eIDAS-Compliant Identity Integration

To enhance age verification, telcos can integrate with eIDAS-notified digital identity systems (e.g., SPID in Italy, FranceConnect+ in France, DigiD in the Netherlands). The proposal is as follows:
- At contract activation, telcos request access to the user's digital identity via an eIDAS-compliant provider.
- Only the age attribute is shared, not full identity data.
- The verified age is associated with the contract and MSISDN.
- For non-SIM-based lines (e.g., fixed broadband, IoT), the system links the line to either a verified SIM/MSISDN with known age or a session-based eIDAS identity assertion.

3.3 Platform-Based and Device-Based Methods

Other methods include:
- Self-declaration (low assurance).
- Document upload (high assurance, privacy-invasive).
- Device-based estimation (AI-driven, prone to bias).
- Zero-knowledge proofs (privacy-preserving, emerging).

3.4 Telco-Enabled Age Verification Interfaces

To support privacy-preserving and scalable age-based access control, telcos could offer an API interface that allows applications and platforms to query whether a user is above or below a specific

age threshold (e.g., over 13, over 18), without revealing the user's exact age or identity. This binary response model minimizes personal data exposure while enabling compliance with content access regulations. Additionally, operating systems could implement an entitlement mechanism that periodically requests age verification from the user's Internet Service Provider (ISP). This entitlement would be valid for a limited duration (e.g., refreshed every 30 days), ensuring that age status remains current while avoiding constant re-authentication. Such mechanisms would allow for seamless integration across apps and devices, while maintaining user privacy and regulatory alignment.

The CAMARA project is developing such an API : Know Your Customer – Age Verification . Onje benefit of an API-driven approach is that the request to verify a customer's age, and the resulting response, are traceable by the telco and the adult service provider calling the API. This provides an audit trail to show that the adult service provider made a check and received a valid response before granting the end user access to their service.

These can complement telco-based verification in a multi-layered architecture.

4. Blocking Mechanisms for Age-Based Restrictions

Telcos and platforms can implement content access restrictions using various technical mechanisms:

4.1 DNS Filtering

- Blocks access to domains listed as inappropriate.
- Easy to deploy but vulnerable to circumvention.

4.2 IP/Domain-Based Blocking at Network Level

How it works: Traffic to specific IPs or domains is blocked at the network gateway.
Pros: More robust than DNS filtering.
Cons: Risk of overblocking, especially with shared hosting or CDNs.
Impact of ECH: With the deployment of Encrypted Client Hello (ECH), the Server Name Indication (SNI) in TLS handshakes is encrypted. This significantly reduces the visibility of domain names in network traffic, making it harder for IP/domain-based blocking to accurately identify and filter specific services hosted on shared infrastructure. As a result, reliance on IP-based blocking may lead to increased collateral damage or ineffectiveness, especially when multiple services share the same IP address.

4.3 HTTP/HTTPS Interception (Deep Packet Inspection)

How it works: Inspects traffic content to enforce restrictions.
Pros: Offers fine-grained control.
Cons: Raises significant privacy and legal concerns, especially with encrypted traffic.
Impact of ECH: ECH encrypts the SNI and other parts of the TLS handshake, limiting the ability of DPI systems to inspect or classify traffic based on domain names. This reduces the effectiveness of DPI

for domain-level filtering and may necessitate alternative approaches such as endpoint cooperation, client-side enforcement, or metadata-based classification.

4.5 SIM/MSISDN-Based Access Control

- Age status tied to the SIM, enabling telco-level enforcement.
- Can be used to gate access to services or content platforms.

5. Curation of Blocking Lists

Blocking lists are central to any access control system. Their governance and accuracy are critical.

5.1 Sources

- Regulatory mandates (e.g., gambling, adult content).
- Industry consortia (shared lists across providers).
- AI/ML classification (automated tagging).
- User/community reporting (crowdsourced moderation).

5.2 Curation Principles

- Transparency: Clear inclusion/removal criteria.
- Appeal mechanisms: Allow content providers to challenge listings.
- Jurisdictional awareness: Reflect local laws and cultural norms.
- Update frequency: Regular reviews to maintain relevance.

5.3 Implementation Models

- Centralized: Managed by a single authority.
- Federated: Shared governance across stakeholders.
- Decentralized: Each provider maintains its own list with metadata standards.

6. Geographic Differences in SIM Registration

In most European countries, identity verification is mandatory for prepaid SIM purchases:
- Countries with mandatory registration: Italy, France, Germany, Spain, Belgium, Greece, Poland, Austria, etc.
- Countries with partial or voluntary registration: UK, Ireland, Sweden, Denmark.
- Trend: Movement toward universal registration across the EU for security and regulatory compliance.

This regulatory landscape makes telcos in Europe particularly well-positioned to support age-based access control.

7. Corner Cases and Mitigations

Corner Case	Risk	Mitigation
Shared Devices	Minors bypass restrictions	Multi-profile support, session-based prompts
SIM bought by parent for child	Incorrect age attribution	User assertion, linked accounts
Prepaid SIMs (in countries without ID checks)	Weak identity linkage	Default restrictions, incentivized registration
SIM swapping	Age status mismatch	SIM-device binding, re-authentication
Roaming	Jurisdictional mismatch	Geolocation-aware policies
Corporate SIMs	Unknown user age	Enterprise declarations, policy APIs
Non-SIM lines	No age linkage	Session-based eIDAS assertion or SIM association

8. Governance and Interoperability

Effective implementation requires collaboration across:
- Regulators: Legal clarity and compliance.
- Telcos and platforms: Technical integration and enforcement.
- Standards bodies: Interoperable APIs and protocols.
- Civil society: Safeguards against misuse and discrimination.

Privacy-preserving technologies should be prioritized to minimize data exposure while maintaining effectiveness.

9. Recommendations

- Standardize age assertion protocols across telcos and platforms.
- Integrate eIDAS-compliant identity systems for verified age sharing.
- Promote interoperable APIs for age verification and content control.
- Support privacy-first architectures using decentralized identity and zero-knowledge proofs.

- Establish transparent governance for blocking lists.
- Align blocking mechanisms with jurisdictional requirements, especially in roaming scenarios.
- Encourage multi-layered verification models combining SIM-based, platform-based, and session-based controls.

10. Conclusion

Telcos are uniquely positioned to contribute to age-based access restrictions through verified identity, persistent identifiers, and network-level enforcement. By integrating eIDAS-compliant identity systems and supporting session-based age assertions, telcos can enable scalable, privacy-conscious solutions that respect geographic and regulatory diversity.