Compliance with IEEE Standards Policies and Procedures

Subclause 5.2.1 of the *IEEE-SA Standards Board Bylaws* states, "While participating in IEEE standards development activities, all participants...shall act in accordance with all applicable laws (nation-based and international), the IEEE Code of Ethics, and with IEEE Standards policies and procedures."

The contributor acknowledges and accepts that this contribution is subject to
- The IEEE Standards copyright policy as stated in the *IEEE-SA Standards Board Bylaws*, section 7, http://standards.ieee.org/develop/policies/bylaws/sect6-7.html#7, and the *IEEE-SA Standards Board Operations Manual*, section 6.1, http://standards.ieee.org/develop/policies/opman/sect6.html
- The IEEE Standards patent policy as stated in the *IEEE-SA Standards Board Bylaws*, section 6, http://standards.ieee.org/guides/bylaws/sect6-7.html#6, and the *IEEE-SA Standards Board Operations Manual*, section 6.3, http://standards.ieee.org/develop/policies/opman/sect6.html

◆IEEE

IEEE P2089.1
Standard for Online Age Verification

Online Age Verification		
Date: 2021-12-08		
Author(s):		
Name	**Affiliation**	**E-mail (Optional)**
I Corby	AVPA	iain@avpassociation.com

IEEE

Contents

IEEE

1. Overview

1.1. Scope

This standard is the second in a family of standards focused on the 5Rights principles and establishes a framework for the design, specification, evaluation and deployment of age verification systems. It includes;

1. the key terms, definitions and abbreviations, together with the roles and responsibilities of key actors in the age assurance process,
2. requirements for establishing different levels of confidence (asserted, standard, enhanced and strict) associated with the types of age assurance systems,
3. requirements for privacy protection, data security and information systems management that are specific to the age assurance process.

It does not specify

1. detailed information about countermeasures (i.e. anti-spoofing techniques), methods to detect presentation attacks, algorithms, or sensors;
2. methods to assess the overall system-level security or vulnerability

The framework centers around the following key areas as follows:

— Roles and responsibilities of key actors in the age assurance process

— Determining the need for age verification

— Selecting the method of age verification

— Verifying the age of a user

— Categorising the level of confidence with which the verification has been completed

— Exchanging the results of age verification checks with other organizations

— Protecting the privacy of users when undertaking age verification

— Securing data relating to users used when undertaking age verification

— Considering the capacity of and upholding the rights of children

— Presenting information about age verification in an age appropriate way

This standard provides specific levels of confidence and evaluation criteria and explains how Age Verificaton providers and organizations can meet the criteria.

Data privacy and security are complex and highly regulated areas of law, particularly as related to children and young people. The relevant legal definitions and requirements are rapidly evolving, and may vary at the local, state, national, and regional level. No standard can provide unconditional consistency with all such laws and regulations. Users of this standard are responsible for referring to and observing all applicable legal and regulatory requirements, and should refer questions of compliance to competent legal counsel with expertise in the relevant jurisdiction.

1.2. Purpose

This standard provides a set of processes for digital services to ascertain the age of a user, to a proportionate degree of accuracy and certainty, when offering age-restricted or age-appropriate content, goods or services. This is essential to creating a digital environment that supports, by design and delivery, children safety, privacy, autonomy, agency, and health, specifically providing a set of guidelines and best practices and thereby offering a level of validation for service design decisions.

1.3. Use of the standard

The standard describes the set of processes by which leaders, managers, engineers and technologists can undertake online age verification.

It provides implementable processes to help align innovation management to make processes, system design approaches, and software engineering methods age appropriate and, in doing so, reduce risk and, wherever possible, amplify the benefits of the digital world for end users under the age of 18.

The standard sits on the values of 5Rights Foundation's principles and reflects the rights of children under the United Nations Convention on the Rights of the Child. Many digital systems impact children in intended or unintended ways and, therefore, should take them into account. All organizations for which that is the case are encouraged to use this standard to help make that engagement age appropriate. This standard can be used to ensure children's access to the internet is managed in an age-appropriate manner.

Before using this standard, it is necessary to consider that your product or service is likely to be accessed by children or engage with children either directly, indirectly, deliberately or accidentally in the course of their operations. Data analytics, independent research, research about similar services and products, or research from surveys and research with children may help identify if and how your products, services, or systems engage with children and/or their data. In each case, if children use your services and/or if you collect children's data; this standard aims to help organizations limit access to services that are unsuitable for children of a certain age or, conversely, should be restricted for use only by children in a qualifying age group. This standard is based on the foundation that the 'best interests' (see Clause 3) of the child are placed in primary focus during the design of digital services.

To reach this goal, this standard supports organizations in ascertain whether age verification is required, and if so, how best to implement it. It is applicable within any life cycle model or set of methods for systems and software engineering and/or new or modified product or service development including brokering children's data. If organizations have running systems that cause risks to children, then the processes in this standard can be used for reiteration of analysis and redress.

1.4. Process overview

The goal of this standard is to enable organizations to limit access to their services to suitable age-groups, with the rights and needs of children in mind. Age appropriateness includes a variety of values that support children. For example, values such as sustainability, privacy, usability, convenience, controllability, accountability, inclusivity, evolving capacity, and children's rights can be implemented by this standard. This standard also supports values or attributes in systems typically considered in system engineering, such as functionality, efficiency, and effectiveness. An overview of the key processes in this standard is depicted in Figure 1.

◆IEEE

Figure 1 – Key Processes

| Determining the need for age verification | Selecting the method of age verification | Verifying the age of a user | Categorising the level of confidence with which the verification has been completed | Exchanging the results of age verification checks with other organizations | Protecting the privacy of users when undertaking age verification | Securing data relating to users used when undertaking age verification | Considering the capacity of and upholding the rights of children | Presenting information about age verification in an age appropriate way |

1.5. Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals is *required to*)[12]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (should equals is recommended that).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals is permitted to).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals is *able to*). 2.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they shall be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO Guide 73:2009, Risk management—Vocabulary.[3]

ISO 9000:2005, Quality management systems—Fundamentals and vocabulary. [1]

The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations. Figure 1—Relationship of processes and stages in IEEE Std 2089-2021

---

[1] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

[2] [2]The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact. [3]ISO publications are available from the ISO Central Secretariat (https:// www .iso .org/). ISO publications are also available in the United States from the American National Standards Institute (https:// www .ansi .org/).

ISO 9000:2015, Quality management systems—Fundamentals and vocabulary.

ISO/IEC 25010:2011, Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models. ·[4,5]

ISO/IEC/IEEE 15288:2015, Systems and software engineering—System life cycle processes.[6]

ISO/IEC/IEEE 15289:2011, Systems and software engineering—Content of life-cycle information products (documentation).

ISO/IEC/IEEE 29148:2018, Systems and software engineering—Life cycle processes—Requirements engineering.

ISO/IEC/IEEE 42010:2011, Systems and software engineering—Architecture description.

UNCRC General Comment No. 14, Para.4, General Comment No. 5, Para. 12 CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12).[7]

United Nations Convention on the Rights of the Child (UNCRC), 1989.[8]

United Nations Committee on the Rights of the Child General Comment (25), 2021 on Children's Rights in Relation to the Digital Environment.[9]

Universal Declaration of Human Rights (General Assembly resolution 217 A), United Nations General Assembly, 10 December, 1948 .[10]

 U.S. Code 230—Protection for private blocking and screening of offensive material, US Communications and Decency Act, 1996.

In addition to the normative references listed above, consideration needs to be given to meeting the relevant national and regional legislation and industry standards, in the jurisdictions(s) in which the service or product will be offered, but there are instances where the law does not go far enough and so this standard sets the baseline to prioritize the rights of children and may go beyond the requirements of the law. See also Annex E for examples of regulations at the time of publication of the standard.

[4]ISO/IEC publications are available from the ISO Central Secretariat (https:// www .iso .org/). ISO/IEC publications are available in the United States from the American National Standards Institute (https:// www .ansi .org/).

[5]IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (https:// standards .ieee .org/).

[6]The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

[7]Available at: https:// www2 .ohchr .org/ English/ bodies/ crc/ docs/ GC/ CRC C GC 14 ENG .pdf.

 [8]See https:// www .ohchr .org/ en/ professionalinterest/ pages/ crc .aspx.

[9]Available at: https:// tbinternet .ohchr .org/ layouts/ 15/ treatybodyexternal/ Download .aspx ?symbolno = CRC %2fC %2fGC %2f25 & Lang = en.

[10]Available at: https:// www .un .org/ en/ development/ desa/ population/ migration/ generalassembly/ docs/ globalcompact/ A RES 217(III) .pdf.

IEEE

3. Definitions, acronyms, and abbreviations

3.1. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [11]

acquirer: A stakeholder that acquires or procures a product or service from a supplier. NOTE—Other terms commonly used for an acquirer are buyer, customer, owner, purchaser, or internal/organizational sponsor.[12]

acquisition: The process of obtaining a product, service, or system.

activity: A set of cohesive and purposeful tasks of a process.

age appropriate: Something that is suitable or appropriate for a person of a particular age. This concept is often, but not exclusively used in relation to children—a demographic who develop rapidly over a short space of time. NOTE—In the digital context, the concept of age appropriate is most associated with the UK's Age Appropriate Design Code that sets out data protection measures to benefit children [B3][13].

age appropriate register: An information repository created for clarity, unambiguity and traceability reasons for your product or service that contains data and insights gained in child impact exploration, prioritization, and traceability into product/service requirements.

age assurance: An umbrella term for both age verification and age estimation solutions. The word "assurance" refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

age estimation: A process that establishes a user is likely to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include automated analysis of behavioral and environmental data, comparing the way a user interacts with a device with other users of the same age, and metrics derived from motion analysis or by testing their capacity or knowledge.

age verification: A system that relies on hard (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish age only.

agreement: Mutual acknowledgment of terms and conditions under which a working relationship is conducted, for example, a contract or memorandum of agreement.

architecture: See ISO/IEC/IEEE 42010:2011.[14]

assurance: The word "assurance" refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

audit: See ISO/IEC/IEEE15288: 2015.

NOTE—The scope includes professional and industry codes of practice.

FOOTNOTES

[11]*IEEE Standards Dictionary Online* is available at: http:// dictionary .ieee .org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

[12]Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

[13]The numbers in brackets correspond to those of the bibliography in Annex F. [14]Information on references can be found in Clause 2.

balancing: Where one right comes into conflict with another, they should be balanced so that the "best interests" of the child is paramount.

best interest: See: UNCRC General Comment No. 14, Para.4, General Comment No. 5, para. 12. **benefit**: A positive outcome that is voluntarily or involuntarily created by an act, system or process. NOTE—Benefits correspond to one or more underlying desired values.

child: For the purposes of digital services provided within the context of this standard, a child means every human being below the age of 18.

child-centered design: A design approach that prioritizes children's rights and needs in service design and governance, bearing children's best interests at the heart of any design process. **children's rights**: A framework of legal and other obligations and ethical values covering civil, political, economic, social, and cultural rights afforded to every child. NOTE—Documented in the United Nations Convention on the Rights of the Child.

concept of operations: A verbal and/or graphic statement, in broad outline, of an organization's assumptions or intent in regard to an operation or series of operations. **concern**: See ISO/IEC/IEEE 42010:2011.

context of use: Intended operational environment for a system. NOTE 1—The environment determines the setting and circumstances of all influences upon a system, including not only other systems but also people, settings, social, and ecological factors, etc. NOTE 2—Context of use can be captured using a Context of Use Description (See ISO/IEC 25063.3 [B2]).

control: The ability to determine the nature, sequence and/or consequences of technical and operational settings, behavior, specific events and/or experiences. NOTE—Control includes cognitive control; that is being informed about activities; decisional control: having choices over actions; and behavioral control; receiving feedback from actions.

design: (verb and noun) See ISO/IEC/IEEE 15288:2015.

environment: See ISO/IEC/IEEE 42010:2011. NOTE—Also applies to products and services.

ethical: Supporting the realization of positive values or the reduction of negative values. NOTE—In this definition, a system can be ethical or unethical in the sense that it bears value dispositions to cater to positive value creation or negative value prohibition.

evolving capacity: As children acquire enhanced competencies, there is a greater capacity to take responsibility for decisions affecting their lives.

fair terms: A concept that the terms of use for a product or service do not put the consumer at a disadvantage.

functional requirement: A statement that identifies what results a product or process shall produce.

harm: (noun) A negative event or negative social development entailing damage or loss to people.

harm: (verb) Acting with negative value effects for self or others, within a respective product or service, organization, or beyond.

hazard: A condition with a potential for causing harm.

human rights: See Universal Declaration of Human Rights, United Nations General Assembly, 10 December 1948 (General Assembly resolution 217 A).

information item: See ISO/IEC/IEEE 15289:2011.

Level of confidence: to aid clarity, this standard refers to the five defined levels of assurance for the age assurance process as levels of confidence.

life cycle: Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

life cycle model: A framework of processes and activities concerned with the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding.

nonfunctional requirement: A requirement that describes not what the system will do but how the system will do it.

operational concept: See ISO/IEC/IEEE 15288:2015. NOTE 1—The concept of operations is produced at an early conceptual stage in describe system functions and relationships from a user's point of view. The operational concept details how the system will be operated in production. NOTE 2—The operational concept should include all major product, service, or system elements and/or system components, boundaries, and directly adjunct elements beyond boundaries, internal, and external input elements (i.e., databases and/or applications serving the system that may be outside of the product or service's boundaries) and output elements (i.e., databases and/or applications serving the system that may be outside of the product or service's boundaries).

NOTE 3—The operational concept should preferably be visualized.

operator: An individual or organization that performs the operations of a product, service, or system.

NOTE 1—The role of operator and the role of user can be vested, simultaneously or sequentially, in the same individual or organization.

NOTE 2—An individual operator combined with knowledge, skills and procedures can be considered as an element of the service or system.

NOTE 3—An operator may perform operations on a product or service that is operated, or of a product or service that is operated, depending on whether or not operating instructions are placed within the product or service's boundary.

opportunity: A condition or state with a potential to lead to a benefit or gain.

organization: A group of people and facilities with an arrangement of responsibilities, authorities and relationships, for example, corporations, firms, enterprises, institutions, charities, a sole trader, associations, or parts or combinations thereof. NOTE—An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities, and relationships. A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

parent: The legal guardian of a child.

NOTE—For the purposes of this standard, "parent" can mean parents, legal or state appointed guardians, or, in certain limited circumstances, another adult in a position of authority, such as an educator, consistent with all applicable laws and regulations for the relevant jurisdiction.

persona: An archetypal user of a product, service, or system.

NOTE 1—Personas represent the needs of a larger group in terms of their goals, expectations, and personal characteristics. They help to guide decisions about system design and design targets.

NOTE 2—The term "persona" stems from the field of usability design where personas are typically described in a storytelling exercise. Project teams put themselves in the shoes of their potential stakeholders. They bring personas to life by giving them names, personalities, and photos.

problem: A difficulty, uncertainty, or otherwise realized and undesirable event, set of events, condition, or situation that requires investigation and corrective action.

process: See ISO 9000:2005.

product: The result of a process.

NOTE—There are four agreed generic product categories: hardware (e.g., engine mechanical part), software (e.g., computer program), services (e.g., transport), and processed materials (e.g., lubricant). Hardware and processed materials are generally tangible products, while software or services are generally intangible.

program: Related projects, subprograms and program activities managed in a coordinated way to obtain benefits not available from managing them individually.

project: An endeavor with defined start and finish criteria undertaken to create a product or service in accordance with specified resources and requirements.

published terms: *Any* document that sets out rules or basis upon which a child and an organization engage with each other, including but not limited to community standards, terms and conditions, and a privacy notice.

quality assurance: See ISO 9000:2015.

quality management: See ISO 9000:2005.

requirement: See ISO/IEC/IEEE 29148:2018.

resource: An asset that is utilized or consumed during the execution of a process.

NOTE 1—Includes diverse entities, such as funding, personnel, facilities, capital equipment, tools, and utilities, such as power, water, fuel, and communication infrastructures.

NOTE 2—Resources include those that are reusable, renewable, or consumable.

reward: A positive outcome arising from an opportunity.

NOTE 1—Similar but opposite to the concept of risk, reward is characterized by the likelihood of attaining some beneficial outcome and the magnitude of the gain.

NOTE 2—Reward is expressed in terms of combination of the likelihood and extent of a benefit being realized.

◆IEEE

risk: See ISO Guide 73:2009.

NOTE 1—An effect is a deviation from the expected—positive or negative. A positive effect is also known as an opportunity.

NOTE 2—Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

NOTE 3—Risk is often characterized by reference to potential harmful events and consequences, or a combination of these.

NOTE 4—Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. NOTE 5—Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

risk treatment: The process, procedures, methodologies, and means that provide a basis for and facilitate the reduction or elimination of an intolerable risk.

service: The performance of activities, work, or duties. This includes freemium services.

NOTE 1—A service is self-contained, coherent, discrete, and can be composed of other services.

NOTE 2—A service is generally an intangible product.

stage: A period within the life cycle of an entity that relates to the state of its description or realization.

NOTE 1—Sages relate to major progress and achievement milestones of the entity through its life cycle.

NOTE 2—Stages often overlap.

supplier: An organization or an individual that enters into an agreement with the acquirer for the supply of a product or service.

NOTE 1—Other terms commonly used for supplier are contractor, producer, seller, or vendor.

NOTE 2—The acquirer and the supplier sometimes are part of the same organization. **system**: A combination of interacting elements organized to achieve one or more stated purposes. NOTE—A construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, processes and documents; that is, all things required to produce systems-level results.

system characteristic: Attributes or distinguishing features pertaining to a system.

system element: A member of a set of elements that constitute a system. For example, hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities or any combination.

NOTE—A system element is a discrete part of a system that can be implemented to fulfill specified requirements.

14

task: A required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process.

trade-off: A decision-making action that selects from various requirements and alternative solutions on the basis of net benefit to the stakeholders.

top management: A person or group of people who direct and control the organization at the highest level.

NOTE—Top management can be the owner of an organization, majority shareholders, senior manager in the organization, or members of the governing board.

unfair terms: Terms that do not meet the definition of "fair terms."

See also: **fair terms**. **user**: See ISO/IEC 25010:2011.

NOTE—The role of user and the role of operator are sometimes vested, simultaneously or sequentially, in the same individual or organization.

validation: See ISO 9000:2015. NOTE—A system is able to accomplish its intended use, goals and objectives (i.e., meet stakeholder requirements) in the intended operational environment. The right system was built.

value: Something desirable that influences the selection from available modes, means and ends of action. Examples of positive values include love, privacy, security, transparency, accountability, generosity, dignity, courage, and fairness. Examples of negative values include bias, ambiguity, absence of privacy, selfishness, and greediness.

value lead: The person assigned to coordinate and conduct related to value elicitation and prioritization and traceability of values through the requirements and design artifacts.

verification: See ISO 9000:2005.

5Rights Principles: A framework developed with young people by the 5Rights Foundation that sets out five principles that establish children's entitlement in the digital world. This includes the right to remove, the right to know, the right to safety and support, the right to informed and conscious use, and the right to digital literacy.

3.2. Acronyms and abbreviations

AADSF Age Appropriate Digital Service Framework

AAR Age Appropriate Register

CCCM Change Control and Configuration Management

CSEA child sexual exploitation and abuse

UNCRC United Nations Convention on the Rights of the Child

4. Conformance

The processes in this standard allow an organization to construct a life cycle and/or design and develop methodologies appropriate to make its product and services age appropriate.

This standard can be used in one or more of the following modes:

By an organization: to help establish appropriate age verification processes. These processes can be supported by an infrastructure of policies, methods, procedures, techniques, tools, and trained personnel to support the organization to perform and manage its projects and systems through each of their life cycle stages. In this mode this standard is used to assess if the organization's approahc is conducive to effective age verification outcomes.

By an AV provider: to help select, structure, and employ the elements necessary to provide age verification. In this mode, this standard is used to determine the client organization's requirements and assess if the project's outcome is effective in applying age verification.

By an acquirer and a supplier: to help develop an agreement concerning processes and activities that deliver age verification. Via the agreement, the processes and activities in this standard are selected, negotiated, agreed to, and performed. In this mode this standard is used for guidance in developing agreements referring to age verification.

By process assessors: to serve as a process reference model for use in the performance of process assessments that may be used to support organizational process improvement for digital services and products that engage with children.

There is only one criterion for claiming full conformance: full conformance to both outcomes and tasks. Full conformance to outcomes and tasks is achieved by demonstrating that all of the outcomes and the required activities and tasks in [Clauses 7] through [Clause 15] have been achieved. The inputs and outputs shown in clauses [Clauses 7] through [Clause 15] are not requirements except as specifically required in the activities and tasks. The inputs and outputs are demonstrable predictors of the outcome in each process.

5. Key concepts and application <mark>This section needs further re-drafting</mark>

5.1. General application

This standard is usable by organizations that engage in system and software engineering and product and service design and development. This includes in particular:

— Organizations providing services and products that engage with children or are likely to be accessed by or engage with children, either directly, indirectly, deliberately, or in the course of their operations

— Organizations building a new generic or application-specific product, service, or system from scratch that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations

— Organizations implementing a major revision on an existing product, service, or system that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations

— Organizations planning the acquisition of a tailored product, service, or system that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations

— Research organizations (including universities) that build a new product, service, or system from scratch or adapt an existing entity in the course of their research activities that may engage with children or are likely to be accessed by or engage with children either directly, indirectly, deliberately, or in the course of their operations

◆IEEE

5.2. Specified context of use

Many organizations engage with children intentionally, others engage with children in the course of their general activities. Some impact on children without engaging directly with them, and some engage unintentionally. In each case the organization has a responsibility to that child to provide an age appropriate service by applying a proportionate degree of age verification. Applying age verification to a product or service means you take steps necessary to offer a product or service that is designed with child users in mind. [Clause 7] sets out the methodology of interrogating the service from the point of view of the established rights and needs of children and provides any organization a starting point from which to implement age verification.

Systems support values relevant to a context of use. For example, with different contexts (school, game, home, public body) come different considerations and impacts. This standard assumes that systems can apply their methodologies and child-centered values to take specific actions that are relevant across different use contexts.

In addition to this, consideration needs to be given to verify relevant national and regional legislation and industry standards in the jurisdiction(s) in which the service or the product will be offered are met, including the following:

— Data protection regulations, including regulations that protect children's data specifically

— Consumer legislation

— Equality legislation

— Children's acts or legislation that covers treatment of children (for example, education, health, justice)

— Health and safety legislation

— Such regulations and legislation that protect children and promote their rights in any jurisdiction

5.3. The organization

This standard is intended to be used in systems and software engineering and digital services organizations of all types and sizes, whether they apply a hierarchical or a relatively flat organizational model. It is also usable by components of an organization, such as a product development team or a corporate division, although conformance to the standard will likely require participation across organizations in an integrated value/ supply chain. It is intended for local, regional, national, or international use with various cultural values and governance systems. In applying this standard, one person can assume many roles, and one role can be held by numerous individuals or subgroups within the organization. There are no requirements for independence of roles in this standard, but the duties associated with all roles shall be fulfilled.

Design and service provision decisions that impact children are not the sole responsibility of top management, although top management has an undeniable role in setting expectations for organizational values and priorities and establishing control of performance and final outcomes. This standard requires the informed judgment of systems and software engineers while making design decisions about a system under development and may not be left solely to management. Both engineers and others in the organization, including those with responsibility for compliance, can benefit from learning and regularly applying specific processes and methods to apply age verification throughout the life cycle. Just as engineering analyses, decisions, and risk assessments have always involved balancing and trade offs of priorities and values, in this context, engineers participate as the organization balancing and finding solutions for competing interests (e.g., risks/ harms). Although involvement with internal or external experts (e.g, in child rights or child development) may improve outcomes and efficiency, it is not required to engage an expert to conform with the standard.

◈IEEE

5.4. Stakeholders

There may be a wide range of stakeholders involved in the products and services that impact children. Internal stakeholders include the many roles required to commission, develop, build, and market products and services. Primary stakeholders include, for example, a child, groups of children, parents, educators—and often adults. There may be third parties that have specific interests, for example, an owner or developer of an app will have an interest and be affected by an app store's policies and practices, a regulator, a trade association to whom the system owner is accountable, or a data broker or agent that may impact the child in ways that are both visible and unseen. Additionally, there are those who interfere or exploit digital systems, such as hackers, scammers, predators. These groups of stakeholders often have an asymmetric influence on the design of the product. An asymmetric influence means having more power to assert your interests and views. Typically, those connected with the proprietary ownership of the technology are the most influential and the end user may only have the power to reject or accept the product or service in its entirety. In the case of systems that impact a user without their knowledge, for example by obtaining their data from a third party, they may have no influence at all. This power imbalance is particularly acute when the end user is a child. This standard offers a set of processes that engage stakeholders with each other to apply age verification to a product or service in a way that prioritizes the rights and needs of children. The person(s) or company building the product or service can, by following this standard, identify the risks and benefits of their system to children and take steps to mitigate risks, amplify benefits, and keep both under review. This set of processes does not seek to undermine engineering realities, nor does it offer an aspirational or perfect world for children, rather it offers actions that, if followed, will make your product or service conscious of and suitable for the children you engage with. They describe a floor of compliance and not a ceiling of ambition. It is anticipated that smaller or newer companies will seek to adopt or purchase age verification systems built by others. In that instance they should adopt certified products or products that come from trusted sources.

5.4.1. Children as users

Along with these internal stakeholders and the customer, the class of stakeholders that is intrinsic to age appropriate design is the users, in this instance, a child. Users frequently are categorized by the levels or types of system access and permissions they need to perform various tasks, or have services provided to them. These include the hands-on system operators (often agents of the customer) as well as those who benefit from or are harmed by use of the system, both through direct transactions using the system and through its impact on the environment and their culture. The word "users" here also includes those who access a system, whether or not they share data with it beyond the age verification process itself. In the case of children, there cannot be a presumption that they are able to assess the risk or benefits of use of any system nor that providing "more information" is a suitable response to offering an age appropriate service, informing them of their rights, or trying to meet their needs. Nor can it be assumed that all children have a parent or adult in loco parentis who is engaged, literate, skilled or able to act on their behalf. The purpose of the standard is to provide children with only those services and products that consider the vulnerabilities associated with their age and are age appropriate by default. Not all children are the same, and children of different ages, contexts, ethnicity, capacity, and socioeconomic groups may require different levels of support or consideration. By capacity, we mean the cognitive ability to comprehend materials plus the ability to be able to read materials. For example, designers need to take particular care that the system design and algorithms do not unjustifiably favor or select users in certain geographic areas, of certain biometric or demographic characteristics, or based on unvalidated reports and unfairly target or exclude other classes of users.

5.4.2. Who can threaten or support the best interest of the child?

Another class of stakeholders may have interests that oppose the system or may interfere with its use. These include competitors, cybersecurity hackers, or opponents of the organization, system owner, or customer. There is also a significant group of producers and consumers of child sexual abuse material. Other external stakeholders can offer divergent perspectives. Government regulators and external advocacy groups, whose expertise, cultural norms, and values may differ from the system owner, can expose a clash in values or demand a higher bar of safety or benefit for children. These conflicting and often oppositional values may even constrain and/or aid the decisions of the system owners that are a direct threat to the needs, rights, and values of children. To counteract any threats to children, the organization may consider the use of the third party assessors, data brokers, and independent verification and validation contractors. These are other types of stakeholders who can point out flaws or unstated assumptions that have influenced or skewed the organization's

18

ethical choices against the needs, rights, and values of children. This standard helps to identify how internal and external stakeholders, users, opponents, and independent authorities can be treated differently when age appropriateness and risks are evaluated. Information about potential system characteristics and performance and the balance of values and stakeholder interests are rarely shared openly with all stakeholders. Therefore, it is one of the goals of this standard to present a set of processes that helps organizations better understand this obfuscated balance of interests and values.

5.5. Stages and processes

This standard allows any organization, systems developer, or digital services provider to achieve the requirements in this standard by means of their own set of standard system development processes, methods and, practices. This standard has distinct processes which can be applied to systems and software engineering and which relate to the general processes in ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017 (see Annex C).

This standard is intended to be suitable for use by organizations and software projects using iterative approaches and methods as well as in those using other formal engineering approaches.

The activities and tasks in this standard are not sufficient by themselves to produce a product or service. They are intended to be an integral part of an organization's comprehensive approach to managing the development of a product or service.

This standard does not prescribe a sequence of processes within the life cycle model. However, many of the activities and tasks logically apply outputs from other tasks, so there is an inherent sequence of activities that can be applied iteratively. The sequence of the processes is determined by project objectives and by selection of the life cycle model. But to conform to the standard all processes shall be undertaken and achieved.

IEEE

6. Roles and responsibilities of key actors in the age assurance process

6.1. General

There are many roles required to successfully complete the tasks and activities outlined in this standard. The roles and their associated competencies that shall be fulfilled are documented in 6.2. These roles may be assigned to one or many people so long as the workload, competencies, and accountabilities are all met. There is no requirement for a separate team member for each role.

6.2. Role descriptions

6.2.1. Relying Party

The Relying Party is an Information Society Service (ISS) offering goods, services or content to users online.

The responsibilities of the Relying Party include the following:

— Determining the need for age verification

— Assessing the level of confidence

— Selecting an AV Provider

— Working with the AV Provider to implement age verification

— Monitoring the effectiveness of age verification and maintaining conformance with this standard.

6.2.2. Age Verification Provider

The Age Verification Provider is either and internal or external third party supplier of technology to verify the age of an online user.

The responsibilities of the Age Verification Provider include the following:

— Listen to stakeholders and team members to understand concerns and potential solutions rather than jumping to a readily available technical solution

— Develop system/software requirements that enable age appropriate design

— Evaluate alternatives and trade-offs for suitability to the context of operation and the organization's long-term strategy while maintaining the commitment to age appropriate design and the best interests of the child

— Optimize technical solutions to support age appropriate values among a range of system requirements

6.2.3. User

The User is a person wishing to access the Relying Party. They may be of any age, including both children and adults.

The responsibilities of the User include the following:

— Organize, analyze, communicate, and record age appropriate concepts, concerns, activities, and decisions in a project b) Include other stakeholders in an inclusive and timely fashion

— Facilitate discussions and age appropriate-related activities to accompany a project in its design efforts d) Build benefits to children and organization through practices like participatory design

— Apply age appropriate risk evaluation and assessment methodologies for design and development stages

20

— Establish and sustain activities to manage different age appropriate risks and priorities throughout the life cycle g) Manage the formation, updating, and integrity of the Age Appropriate Register (AAR) (see Annex B)

7. Determining the need for age verification

7.1. Purpose

The purpose of this process is to undertake an initial overview of your service or product and identify the statutory, regulatory, contractual and ethical requirement for age verification. It is the first step of this standard.

7.2. Outcomes

When you have successfully implemented the Determination phase, you shall be able to show the following:

— The statutory requirements for the Relying Party in each of the jurisdictions where its users are located

— The regulatory requirements for the Relying Party in each of the jurisdictions where its users are located

— The contractual requirements for the Relying Party arising from any legally-binding agreements it has entered into where age verification is featured

— The ethical requirements of the Relying Party in relation to age verification as determined by the Board or its nominated delegate.

7.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verificatin as follows:

— Identify the applicable statutes and regulations in all jurisdictions where users are located

— Review all contracts to identify any obligations relating to age verification

— Discuss and agree the Relying Party's policy to implement the Board's ethical wishes relating to age verification

— Document the need for age verification with clear cross-referencing to each of the above sources.

7.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Statutes

— Regulations

— Contracts database

— Relevant existing policies of the Relying Party

7.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— An organizational Age Verification Policy Statement

8. Selecting the method of age verification

8.1. Purpose

21

IEEE

The purpose of this process is to select the most appropriate method or methods of age verification. It is the second step of this standard.

8.2. Outcomes

When you have successfully implemented the Selection phase, you shall be able to show the following:

— The methods of age verification the Relying Party will implement to comply with its Age Verification Policy Statement.

8.3. Activities and tasks

The project shall implement the following activities and tasks to select the methods of age verification as follows:

— Identify the level of confidence required

— Assess the availability of user data on which to base age verification

— Select the method or methods of age verification which are most suited to the available data

8.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Existing user data analysis

— Hardware assessment

8.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— Methods of age verification

9. Verifying the age of a user

9.1. Purpose

The purpose of this process is to undertake verification of the age of each user of the Relying Party. It is the third step of this standard.

9.2. Outcomes

When you have successfully implemented the Verification phase, you shall be able to show the following:

— The age of each user accessing age-restricted goods, services or content to the degree of accuracy and with the level of confidence required by the Age Verification Policy Statement

9.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verification as follows:

— Obtain the user data required for the selected methods of age verification

— Complete age verification

— Record result

9.4. Inputs

22

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— User data

— Age Verification Provider technology

9.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— A record of user ages, each associated with a level of confidence

10. Categorising the level of confidence with which the verification has been completed

10.1. Purpose

The purpose of this process is to categorise the level of confidence to which the verification has been completed. It is the fourth step of this standard.

10.2. Outcomes

When you have successfully implemented the Catergorisation phase, you shall be able to show the following:

— The level of confidence the Reyling Party has in the age of each user whose age has been verified

10.3. Activities and tasks

The project shall implement the following activities and tasks to categorise the level of confidence with wich age verification has been completed as follows:

— Assess any existing certification for the age verification providers technology

— Undertake tests for uncertified technology

— Categorise

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Levels of confidence for Age Verification listed in Annex A

10.4. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— A record of the level of confidence for each method of age verification and each user record

11. Exchanging the results of age verification checks with other organizations

11.1. Purpose

The purpose of this process is to allow an age verification provider to exchange the results of an age verification process with another age verification provider. It is the fifth step of this standard.

11.2. Outcomes

When you have successfully implemented the Determination phase, you shall be able to show the following:

— The certification required to allow other AV providers to rely on your age checks

— The ability to export age verification checks

— The ability to import age verification checks

23

11.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verificatin as follows:

a) Receive requests

b) Validate requests

c) Provide Responses

d) Record volumes of requests sent and received by AV Provider

11.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

a) Age verification records

b) Protocols

11.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

a) An API capable of sending and receiving age checks

b) Results of age checks undertaken by other AV Providers

12. Protecting the privacy of users when undertaking age verification

12.1. Purpose

The purpose of this process is to ensure that age verification solutions shall protect the privacy of users by design. It is the x step of this standard.

12.2. Outcomes

When you have successfully implemented the Privacy-by-Design phase, you shall be able to show the following:

— The AV Provider does not record the identity of the relying party in any way which can be associated with the identity of the user

— Relying Parties are not given access to the identity of the user

12.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verification as follows:

— Document the method by which age verification transactions are recorded to confirm that it is not possible for the relying party to identify the user, and it is not possible for the AV Provider to record which relying parties enquired about which of its users.

12.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Age Verification Provider system design documentation

12.5. Outputs

24

IEEE

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— Data Privacy Impact Assessment

13. Securing data relating to users used when undertaking age verification

13.1. Purpose

The purpose of this process is to ensure that any personal data used during age verification or retained after an age verification has been completed is stored securely. It is the seventh step of this standard.

13.2. Outcomes

When you have successfully implemented the Data Security phase, you shall be able to show the following:

— Data minimisation with the only personally identifiable data stored being necessary for the purpose of ongoing age verification

— Data security to industry standards

— User control over their PII

— Evidence that the system is not vulnerable to penetration

13.3. Activities and tasks

The project shall implement the following activities and tasks to ensure the security of personally identifiable information (PII) data as follows:

— Document data flows and stores

— List attack vectors

— Conduct Risk assessment

— Conduct penetration testing

— Complete Mitigation activity

— Monitor ongoing network activity

13.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Statutes

— Regulations

— Contracts database

— Relevant existing policies of the Relying Party

13.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

— An organizational Age Verification Policy Statement

— Penetration test results

14. Considering the capacity of and upholding the rights of children

◈IEEE

14.1. Purpose

The purpose of this process is to ensure that age verification complies with the requirements set out in 2089.

It is the final step of this standard.

14.2. Outcomes

When you have successfully implemented the Determination phase, you shall be able to show the following:

— The statutory requirements for the Relying Party in each of the jurisdictions where its users are located

— The regulatory requirements for the Relying Party in each of the jurisdictions where its users are located

— The contractual requirements for the Relying Party arising from any legally-binding agreements it has entered into where age verification is featured

— The ethical requirements of the Relying Party in relation to age verification as determined by the Board or its nominated delegate.

14.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verificatin as follows:

— Identify the applicable statutes and regulations in all jurisdictions where users are located

— Review all contracts to identify any obligations relating to age verification

— Discuss and agree the Relying Party's policy to implement the Board's ethical wishes relating to age verification

— Document the need for age verification with clear cross-referencing to each of the above sources.

14.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

— Statutes

— Regulations

— Contracts database

— Relevant existing policies of the Relying Party

14.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

c) An organizational Age Verification Policy Statement

15. Presenting information about age verification in an age appropriate way

15.1. Purpose

The purpose of this process is to undertake an initial overview of your service or product and identify the statutory, regulatory, contractual and ethical requirement for age verification. It is the first step of this standard.

15.2. Outcomes

IEEE

When you have successfully implemented the Determination phase, you shall be able to show the following:

—— The statutory requirements for the Relying Party in each of the jurisdictions where its users are located

—— The regulatory requirements for the Relying Party in each of the jurisdictions where its users are located

—— The contractual requirements for the Relying Party arising from any legally-binding agreements it has entered into where age verification is featured

—— The ethical requirements of the Relying Party in relation to age verification as determined by the Board or its nominated delegate.

15.3. Activities and tasks

The project shall implement the following activities and tasks to determine the need for age verificatin as follows:

e) Identify the applicable statutes and regulations in all jurisdictions where users are located

f) Review all contracts to identify any obligations relating to age verification

g) Discuss and agree the Relying Party's policy to implement the Board's ethical wishes relating to age verification

h) Document the need for age verification with clear cross-referencing to each of the above sources.

15.4. Inputs

The following resources constitute a suitable, but neither exhaustive nor normative, suite of the process inputs:

c) Statutes

d) Regulations

e) Contracts database

f) Relevant existing policies of the Relying Party

15.5. Outputs

The following work products constitute a suitable, but neither exhaustive suite of the process deliverables:

d) An organizational Age Verification Policy Statement

27

◈IEEE

16. Age appropriate deployment, operation, upgrade, monitoring, and decommissioning

16.1. Purpose

The purpose of this process is that the product or service is operated, maintained, upgraded, monitored, and decommissioned in accordance with its age appropriate requirements. It allows the project teams to assess the effectiveness of any steps you have taken to address identified hazards and opportunities and to strategize for further improvements of your risk management processes, policies, and practices.

16.2. Outcomes

When you have successfully implemented the Age Appropriate Deployment, Operation, Upgrade, Monitoring and Decommissioning process, you shall be able to show the following: a) Appropriate monitoring that the deployment, operation, maintenance, and upgrades of the product or service are age appropriate b) Any child-related issues observed are noted in the AAR and addressed c) Where necessary, preparations for standard and risk assessment are repeated for newly identified obstacles, unfair terms, hazards, and opportunities d) Disposal and decommissioning are performed in line with age appropriate requirements and guidelines

16.3. Activities and tasks

The project shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the age appropriate design:

a) Monitor the product or service deployment, operation, maintenance and upgrades with a view to age appropriate requirements. This activity consists of the following tasks:

1) Evaluate whether the product or service has been deployed in consistence with the requirements in the AAR and define a baseline and record in the AAR. 2) At regular intervals, determine whether the product or service is operated, maintained and upgraded in accordance with age appropriate requirements in the AAR.

NOTE—The organization should specify the intervals of revisiting the system in co-operation with stakeholders.

b) At regular intervals, collect field data and stakeholder feedback and analyze the product or service with a view to the following criteria:

1) The age appropriate risk treatment options implemented retain their effectiveness in the contexts of application.

2) New age appropriate aspects at risk are recognized and addressed in the subsequent redesign or adaptation of the product or service before re-deployment.

3) In the event of inadequacy of risk treatment options, consult stakeholders and either strengthen these or identify new treatment options to maintain the protection demand for each age appropriate requirement in the product or service.

c) Properly dispose of the product or service. This activity consists of the following task: verify that no children rights, data, or privacy aspects are undermined when disposing of or taking the system out of service, consistent with applicable laws and regulations.

d) Record lessons learnt in the AAR.

NOTE—If feasible within corporate practice, make lessons learnt available for other organizations.

NOTE—The monitoring is particularly relevant to data driven services and systems and those with emergent behaviors due to machine learning or adaptative behavior.

16.4. Inputs

The following resources constitute a suitable but neither exhaustive nor normative suite of the process inputs: a) A functional system designed incorporating age appropriate requirements. b) A product or service concept of operation. c) Intended and potential context(s) of system use. d) An AAR for product or service.

16.5. Outputs

The following work products constitute a suitable but neither exhaustive suite of the process deliverables: a) Refined concept of operation b) Updated AAR for the product or service life cycle maintenance by the relevant duty holders c) Updated Case for Age Appropriate Conformity