1 INTRODUCTION

1.1 MINORS TRUST FRAMEWORK GOAL

The goal of the Minors Trust Framework (MTF, Framework) is to create a growing federation of participating organizations and consumers working together to assure greater Child safety, parental empowerment, regulatory compliance, and consumer access and privacy. The MTF embodies the operating rules for the Minors Trust Federation (Federation). Participation in the Federation allows service providers to build a deeper level of trust with Parents, create higher brand recognition, and richer engagement with its audience.

1.2 ALIGNMENT WITH THE NSTIC GUIDING PRINCIPLES

The MTF is informed by of the four Guiding Principles set forth in the National Strategy for Trusted Identities in Cyberspace (NSTIC). Identity solutions will be:

- Privacy-enhancing and voluntary;
- Secure and resilient;
- Interoperable; and
- Cost effective and easy to use.

MTF alignment with the NSTIC Guiding Principles addresses a gap in the current marketplace and helps protect families by raising the bar on security and privacy. As the Identity Ecosystem continues to grow with NSTIC-aligned participants, a positive network effect will be created to the benefit of MTF Users through the interoperability of credentials and an equivalence of strong privacy and security protections. The MTF is intended to be the ‘anchor tenant’ for families within the Identity Ecosystem.

1.3 COMMONLY USED TERMS

The following non-exhaustive list contains terms used commonly throughout the MTF document. The terms in this list are defined more thoroughly throughout the Framework, including in the Glossary found at the end of this document.

<table>
<thead>
<tr>
<th>Commonly Used Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessor Assessors determine whether prospective or current MTF participants are in compliance with the standards and policies set forth in the MTF.</td>
</tr>
<tr>
<td>Attribute Authority (AA) Attribute Authorities verify any number of attributes that can be used to identity-proof a User or confirm a relationship (such as between a Parent and their Child).</td>
</tr>
<tr>
<td>Children’s Online Privacy Protection Act (COPPA) COPPA is a U.S. law created to protect the online privacy of children under 13 (U13). In short, it requires verifiable parental consent for the collection or use of any personally identifiable information of U13s gathered from them online. It also sets out requirements for privacy policies, and responsibilities of online service operators who market to children.</td>
</tr>
<tr>
<td>Child A Child is a person under the age of 13 years, and covered by the Children’s Online Privacy Protection Act (COPPA).</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Consent Management Authority (CMA)</th>
<th>Consent Management Authorities manage consent by parents, guardians or other authorized Adults for Minors to use a Relying Party’s online service or specific features or functions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Service Provider (CSP)</td>
<td>Credential Service Providers deliver registration, verification, compliance and information services for issuing and acceptance of MTF credentials by MTF Members. In its role, CSPs may register Users and issue a credential to Users to enable access to Relying Party services.</td>
</tr>
<tr>
<td>Delegated Adult</td>
<td>A Delegated Adult is an adult chosen by the Child’s Parent who may also grant consent for the Child, such as a second parent, grandparent, or a care provider. The Delegated Adult may not change Child attributes or cancel a credential.</td>
</tr>
<tr>
<td>Dispute Resolution Service Provider (DRSP)</td>
<td>Dispute Resolution Service Providers deliver an effective redress mechanism for individuals who feel their personal information, or that of their Child/Minor may have been misused or disclosed to unauthorized parties.</td>
</tr>
<tr>
<td>Federated Identity</td>
<td>A Federated Identity is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.</td>
</tr>
<tr>
<td>FERPA</td>
<td>The FERPA (Family Educational Rights and Privacy Act of 1974) is federal legislation in the United States that protects the privacy of students' personally identifiable information (PII). The act applies to all educational institutions that receive federal funds.</td>
</tr>
<tr>
<td>Identity Ecosystem</td>
<td>The Identity Ecosystem is an online environment where individuals and organizations are able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices.</td>
</tr>
<tr>
<td>Identity Provider (IdP)</td>
<td>Identity Providers verify identity by determining that an asserted User is who they say they are. This may be accomplished by comparing information provided by the User or Relying Party with information uniquely or not generally known and maintained by the IdP; as well as assessable to the IDP.</td>
</tr>
<tr>
<td>Institutional Credential</td>
<td>An Institutional Credential is for a non-Parent adult who is authorized by an accredited educational institution or a non-educational institution (e.g., Boy/Girl Scouts, 4H, libraries, etc) to grant consent under COPPA, on an institutional basis.</td>
</tr>
<tr>
<td>Minor</td>
<td>A Minor is a person that has not reached the age of majority in the jurisdiction that they reside.</td>
</tr>
<tr>
<td>Parent</td>
<td>A Parent is an adult who is legally responsible for a specific Child or Minor, and may contract for them on their behalf. For the purposes of the MTF, only one responsible adult may have a Parent credential, and may include grandparents and legal guardians. Only the Parent may change the Child’s attribute information or cancel the credential.</td>
</tr>
<tr>
<td>Relying Party (RP)</td>
<td>Relying Parties are online services, merchants and others who agree to accept a federated credential issued by an MTF CSP. RPs comply with legal, technical, and operating practices and procedures as specified by</td>
</tr>
</tbody>
</table>
1.4 MTF GOVERNANCE

The MTF is enforced, modified and promoted through the Generational Trust Alliance ("Foundation"), a Delaware LLP funded through Member fees, grants and sponsorships. The Foundation’s Board of Directors (dark blue layer) will set up three sub-sets of the Board: Advisory Committees, an Onboarding Committee, and an Ombudsman (green layer).

Advisory Committees may consist of Operational, Privacy, Security, and Assessment Policy sub-committees (purple layer) which would oversee the technical, operational, and legal requirements for any organization seeking to operate within the Federation. For example, technical requirements would include security protocols, system configuration, settings, and protocols. Operational requirements would address asset management, access control, and systems recovery. Legal requirements would incorporate known child privacy laws (ie COPPA, FERPA, The Pledge, etc) and fair information standards and practices.

The Onboarding Committee would oversee the recruitment, assessment, and intake of new Federation Participants. The Onboarding Committee will also maintain a registry of all RPs in good standing that CMAs may use as a reference tool.

The Ombudsman would oversee the Dispute Resolution Service Providers and help to address any complaints brought to the board either by Participants or the general public. The light blue layer in the above organizational chart explains who would be amenable to the jurisdiction of the subcommittees. It should be noted that the final governance model will be approved by the seated Board.

<table>
<thead>
<tr>
<th>Student Digital Privacy Pledge</th>
<th>The <strong>Pledge</strong> was introduced to safeguard student privacy regarding the collection, maintenance, and use of student personal information. The Pledge was developed by the FPF and SIIA with guidance from the school service providers, educator organizations, and other stakeholders following a convening by U.S. Representatives Jared Polis (CO) and Luke Messer (IN).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teen</td>
<td><strong>A Teen</strong> is a person between 13 years of age and the legal age of majority for their jurisdiction. They are not currently covered by COPPA. As a student their FERPA directory information is covered.</td>
</tr>
</tbody>
</table>
Organizations (not including Consumers) wishing to participate in the Federation are required to become and remain members in good standing of the Foundation, as described in the Federation Operating Policy and Procedures (FOPP). The Foundation is responsible for promoting adoption of the MTF, maintaining assessment guidelines for Federation Participants, verifying assessments, and enforcing adherence to the MTF.

An additional governance layer within the MTF is comprised of Dispute Resolution Service Providers (DRSPs). DSRPs provide an effective redress mechanism for participants who feel their personal information, or that of their Child may have been misused or disclosed to unauthorized parties. An extensive discussion of a Parent’s remedy can be found in the federation operating principles.

2 MINORS TRUST FRAMEWORK: STRUCTURE

2.1 MTF General Description

The MTF is an online identity trust model, developed in conjunction with the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative aimed at helping individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation. The Federation’s unique role is in helping organizations adhere to the unique requirements around minor’s access and interaction with online information; as well as enable more efficient and privacy enhancing means to conduct transactions with families. It does this by having a complete set of technical, operational, and legal policies that all Federation members adhere to in order to protect minors and their parents’ identities and personal information in a secure, privacy enhancing manner.

Today under COPPA, parents have to separately answer each consent request they get from every online service their kids want interactive access to, which can be a burden for both the parent and the online service provider. Because of this, fewer than 1-in-10 consent requests are acted upon, which frustrates online service providers. The real problem arises, however, when children subvert the process by lying about their age in order to access services. This reinforces the harmful notion that lying is an acceptable practice, as well as putting children at risk of privacy harms and Relying Parties at risk of running afoul of COPPA.

The MTF seeks to remedy this problem. Operating under the rules set by the MTF and promulgated by the Foundation, credential service providers (CSPs) can create an online credential for parents and children that can be used by other online service providers – known as Relying Parties (RPs) – who agree to the high standards of privacy and security under the Federation. The process is both free and simple to use: parents will have their identity verified once by an Identity Provider (IdP), and then be able to pre-consent their kids’ access to Federation-approved online services.

**MTF Policies include:**
- Federation Operating Policy and Procedures (FOPP) Documentation;
- Service provider certifications at multiple levels of assurance;
- Interoperable policies, protocols and reference implementation allowing identity verification services, attribute providers, and credentialing authorities to engage with Federation members;
- A broad array of identity ecosystem participants fostering adoption that represent millions of parents and children; and
- Oversight by the Generational Trust Alliance.

The creation of the MTF and the Federation-compliant identity credentials benefits not only online sites and services directed to children and families, but the entire Identity Ecosystem:
• **Child-directed online services** and their users and parents benefit from streamlined COPPA compliance, greater reliability of user age, increased confidence in parental identity, which all leads to significantly higher conversion rates;

• **General audience online services and apps** benefit in that they have greater opportunity to engage with children in an age appropriate manner rather than reflexively barring their participation due to COPPA;

• **Age restricted product and service providers** can avoid interacting with minors;

• **Other compatible trust frameworks** can off load ID verification of minors to Federation-approved operators, as well as also accept Federation credentials, allowing children to enter the larger Identity Ecosystem when appropriate.

The greatest beneficiary of the MTF will be kids. Today they’re not just being forced to lie about their ages, they’re being excluded from, and marginalized in, online activities of all sorts. Without access to a secure credential that allows them to do the things in which they are permitted, kids are unnecessarily and unjustifiably excluded from experiencing much of the World Wide Web. Online services signing on to the Federation will enable participating children to be full Internet citizens in good standing, work within the law, and enjoy what benefits the Web has to offer them – in a safe and privacy-preserving manner.

2.2 MTF Technical Description

The MTF is the collection of legal, technical, and operational policies that underpin trust across service providers and consumers that conduct transactions online. Federation Participants issue federated credentials to Adults and Children so that the Adult may grant verifiable parental consent to Federation and COPPA certified online services. The MTF enables Credential Service Providers that issue a Child-unique pseudonymous identifier to interoperate and interact with RPs and other Members.

In a federation scenario, when someone attempts to access a protected Service Provider site an Identity Provider is asked to provide information called "identity attributes" to the Service Provider. Attributes might include a unique identifier (traditionally a "user ID") or other information such as organizational affiliation, status, email address, etc. In many scenarios, identity attributes are very useful to Service Providers for access control, personalization, and other purposes. The Federation encourages the support of identity attributes by its participants to improve the COPPA consent process and to help protect personal privacy. The Federation allows the verification of a Parent’s attributes, including their self-asserted association to the Child, and provides the Parent with a unique identifier/relationship link and tools to manage multiple consents, notifications, and associations.

The MTF enables Parents to view their Child’s data and permissions across multiple venues, but prohibits Federation Members from assisting each other in tracking either Children or Parents by both MTF policy and technical enforcement due to the use of unique GUIDs. Credential holders are encouraged to have unique display names available at the online service level. CSPs and CMAs are permitted to maintain information about a User on multiple venues in order to support the use of federated credentials and consent.

The MTF empowers Parents to determine when they transfer control of the Parent-authorized credential to a Minor once they age out of COPPA protections. Minor’s rights to control their credential will be determined by relevant law and the issuing CSP/RP Terms of Service or EULA, and may be viewable from the CMA’s parent portal.
When a Child seeks to access a COPPA-regulated site or online service for the first time, they may be asked for their age. If the Child is, or presumed to be, under 13, they are then asked for their parent-linked online identifier to initiate the COPPA consent process. If the Parent wishes to sign up for an MTF Credential (in this case provided by a Federation Participant acting as both the CSP and CMA), they give their sign-up information and proof of identity via IdP, which can be, for example, the last four digits of their SSN, driver’s license, or credit card. When the IdP reports back a positive verification of the Parent, the CSP/CMA can now create and issue the Federation-compliant identity credential to the Parent. At that point, the Parent may associate their credential with each of their Children, and begin to grant consent to each Federation-compliant online service they wish. Once consent has been granted, the Child is now able to interact directly or access the online service.

2.3 USER SEGMENTS

Federation, Individual and Participant user segments and roles are defined in the following sections. COPPA consent requirements are dependent upon which user segment an organization falls under, and is thus core to both COPPA’s enforcement and the MTF’s consent management function.
2.3.1 **INDIVIDUAL USERS**

Children, Minors, Parents, Educators, and Adults who register and are issued a credential by a Federation CSP are Users who engage Federation Participants through an End User License Agreement (EULA) or Terms of Service (TOS) Agreement that defines responsibilities and obligations among the parties. Individual Users are not signatories to the Federation.

2.3.2 **CHILD-DIRECTED WEBSITES, APPS AND ONLINE SERVICES**

Commercial, non-commercial, and governmental organizations providing online services (including mobile) that are focused all or in part on the U13 audience. Under the Federal Trade Commission Children’s Online Privacy Protection Rule (COPPA Rule) criteria, many services could be described as being directed to Children, regardless of whether they target or intend Children to be their primary audience or not. Both COPPA and MTF requirements for these Participants are further explained in the MTF Credentials section of this document.

### 2.3.2.1 Child-Directed, Children as Primary Audience

Websites and/or online services are determined to be Child-directed, with Children as their primary audience, by considering its subject matter, visual content, use of animated characters or Child-oriented activities and incentives, music or other audio content, age of models, presence of Child celebrities or celebrities who appeal to Children, language or other characteristics of the web site or online service, as well as whether advertising promoting or appearing on the website or online service is directed to Children. For websites and online services where Children are the primary audience, age-gating is not permitted. An age-gate is a system used by an online service or app to confirm via self-assertion of age that the user attempting to access their service is of the age required (usually by law) to view the service’s content.

### 2.3.2.2 Child-Directed, Children Not Primary Audience

Websites and/or online services that are directed at Children, but do not target Children as their primary audience are not deemed directed at Children if it does not collect personally identifiable information from any visitor prior to collecting age information. In addition, the service prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of the COPPA Rule. The COPPA Rule further establishes that websites and/or online services where Children are not the primary Audience may use age-gating to determine the age of the User and provide COPPA protection only to those users under the age of 13. Note that sites or services directed to children cannot use the age screen to block children under age 13.

### 2.3.2.3 General Audience Websites and Online Services

General Audience organizations serve a wide demographic but do not specifically target the U13 audience. However, many of these organizations, inclusive of third party ad networks, mail vendors, tools, may engage Children who register under false pretenses to participate in social media or other activities not intended for Children or Minors without consent. General Audience websites or online services are deemed directed to Children when it has actual knowledge that it is collecting personal information either directly, or from users of another website or online service directed to Children. General Audience organizations may wish to reduce potential liability by using CSPs and/or CMAs to determine if a potential User is a minor. A general audience service which utilizes an age gate may choose to block a child’s access entirely.

2.3.3 **AGGREGATORS**

Mobile and cable carriers, social media platforms, and device manufacturers provide broad national coverage across multiple digital domains and venues. Aggregators enroll consumers into their services while collecting

---

2. 16 C.F.R. § 312.2.
attributes necessary for the provisioning of their services, including billing information. They may provide parental identity and permission services for users accessing Child directed content through RPs that utilize the services. They may also provide IdP, CMA and AA services.

2.3.4 Restricting Access to Adult Content
These organizations include online services that are aimed at Adults (such as e-Commerce sites where Children cannot contract), as well as purveyors of mature content, where Children’s registration or engagement would be regarded as inappropriate or illegal. These organizations can ping, discover, and block minor’s access to age-restricted services by utilizing an age-appropriate verification registry available to parents and guardians.

3 Minors Trust Framework Credentials

3.1 Credentials Under the Minors Trust Framework
The MTF certifies a number of different credentials:

- The MTF Parent Credential is for the Parent of a Minor.
- The MTF Delegated Adult is for the second parent or grandparent of a Minor.
- The MTF Young Adult Credential is for young adults 18-20 that are associated with Minor activities.
- The MTF Minor Credential for minors who require access to online services via a login credential. Use of the credential may or may not require parent authorization depending on legal jurisdiction.

An RP may require that Adult consent be needed for participation by Minors 13 and above (e.g., RP requires parental consent for Minors up to 15 years of age). Federation Participants shall try to accommodate such requests.

3.2 MTF Credential Verification Levels and Identity Assurance Program

MTF Credential Identity Assurance Program (IAP): Assertion Profiles & Policy
An MTF Credential Identity Assertion Profile (IAP) specifies a set of criteria that, if met or exceeded by a service provider, provide a useful tool by which a CSP and/or RP might determine whether Assertions of Identity conforming to those criteria can be used to help manage access to its service(s). The MTF defines IAPs to meet the requirements of a community of interested CSPs, RPs, and IdPs specifically those achieving compliance with COPPA, FERPA, and in the future, the Federal Identity, Credential, and Access Management (FICAM) requirements. The MTF intends to minimize the number of profiles by making them applicable to the broadest audience of CSPs, IdPs, and RPs. MTF Assessors have the role of reviewing MTF service provider’s adherence to the IAPs.

3.2.1 The MTF Parent Self Asserted Credential
The MTF Parent Self Asserted Credential requires that the Minor Child or Parent self-asserted identity is REASONABLY verified and the relationship between the Minor Child and Parent REASONABLY established. This is suitable for COPPA’s 'Email Plus' mechanism for obtaining parental consent. Self-Asserted identity and Self-Asserted relationship.
For capturing a Child’s Personal Identifiable Information (PII) for internal use only (no public disclosure or onward transfer). The COPPA approved ‘Email Plus’ mechanism verifies Adults for RPs who collect personally identifiable information (PII) from Minor children only for the RP’s internal use. Email Plus allows a Minor Child or parent -asserted email to be activated via a link, followed by a confirmatory process three days after the account creation.  

3.2.2 THE MTF PARENT VERIFIED CREDENTIAL

The MTF Parent Verified Credential requires that the Parent self-asserted identity is STRONGLY verified and a relationship asserted between a Minor(s) and a Parent is REASONABLY established as detailed by COPPA and Federation Policies. This is suitable for Verifiable Parental Consent under COPPA (FULL VPC). Verification methods REASONABLE in light of current technology include: Full or Partial US SSN; Government issued ID; corporate-issued ID or email verification; credit/debit card transaction that provides notification of each discrete transaction to the primary account holder; phone utilizing trained operator (with or without ID check); print form signed by Adult and returned via U.S. mail, fax, or electronic scan; virtual in-person utilizing trained operator (e.g., Skype); out-of-band SMS in conjunction with known adult phone number; knowledge-based authentication methods (KBA); FICAM LOA 2 (or higher) certificate.

Note: the parent status remains self-asserted. Only Federation Parent Credential holders may change a Minor Child’s attributes or cancel a Minor Child’s credential, or may authorize the association of an Institutional Credential to the Child.

3.2.3 THE MTF PARENT VERIFIED PLUS CREDENTIAL

The MTF Parent Verified Plus Credential requires that the Minor or Adult-asserted identity is STRONGLY verified and the relationship between the Minor Child and Adult is STRONGLY established. Strong verification requires at least two of the above referenced methods used in the MTF Verified Credential. These credentials will be suitable for use in applications that require a higher level of identity proofing, such as financial transactions or the handling of healthcare information.

For sharing or public disclosure of Children’s PII (or some RPs may require for Minors 13+). COPPA requires higher levels of identity assurance, which the MTF recognizes as ‘Verified.’ While COPPA requires the Adult’s self-asserted identity be verified, The MTF Parent Credential: Plus requires STRONG identity verification, which requires two methods of verification to assure identity, as well as the relationship between the Edu or an NPO Institutional Credential, as described in MTF Section 3.2.7. Please refer to the non-exhaustive list of methods in Section 3.2.2 that are reasonable in the light of current technology to assure the asserted parent or guardian is an adult. Only Federation Parent Credential holders may change a Child’s attributes or cancel a Child’s credential, or may authorize the association of an Institutional Credential to the Child.

1 The FTC’s “Email plus” allows online service providers (OSP) to request (in the direct notice sent to the parent’s online contact address) that the parent indicate consent in a return message. To properly use the email plus method, OSPs must take an additional confirming step after receiving the parent’s message (this is the “plus” factor). The confirming step may be (1) requesting in the OSP’s initial message to the parent that the parent include a phone or fax number or mailing address in the reply message, so that the OSP can follow up with a confirming phone call, fax or letter to the parent; or (2) after a reasonable time delay, sending another message via the parent’s online contact information to confirm consent. In this confirmatory message, the OSP should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to do so.
Note: if there is a Minor and Adult relationship established in the offline world that can be leveraged to establish the online relationship then this could be utilized to deliver levels of assurance needed for STRONGLY establishing the Minor & Adult relationship for purposes of this credential. For example, the relationship is asserted by a professional person such as a doctor, teacher or educational administrator. Or a parent could provide a copy of a birth record.

3.2.4 **The MTF Delegated Adult Credential**

The MTF Delegated Adult Credential has the same requirements found in the associated MTF Parent Credential. The MTF addresses instances where a Minor Child’s Parent may wish to grant another Parent, grandparent, or responsible adult the ability to provide consent for the Minor to provide personal information to a compliant Federation online service, when seeking pre-approval of the primary Parent for each instance may be impractical.

The **MTF Delegated Adult Credential** enables an additional Parent, grandparent, or responsible adult to grant consent to access online services that are also MTF RPs on behalf of the parent. The MTF adds additional requirements that Parents be given the ability to receive notice, the ability to pre-consent a Minor Child’s access to a service, as well as the ability to opt-out. The identity proofing and attribute verification requirements of the MTF Delegated Adult Credential maybe self-asserted by the Verified Plus parent. MTF Delegated Adult Credential holders may not change a Minor Child’s attributes or cancel a Child’s credential, nor authorize the association of an institutional Credential to a Minor Child.

CMAs and/or RPs will remain responsible for notifying the Parent when consent is granted, provide access to information collected, and disclose all relevant privacy policies to both the Parent/Guardian and the Delegated Adult.

3.2.5 **The MTF Young Adult Credential**

The MTF Young Adult Credential is for young adults 18-20 that are associated with Minor activities. This credential is the same as the Minor Teen credential and can be self-asserted or verified with the same methodologies in 3.2.2 above but cannot manage a child credential.

3.2.6 **The MTF Minor Credential** for minors who require a login credential.

The MTF Minor Credential is for a Minor under the age of 18. It is created automatically when a Minor initiates the creation of a login credential. If the Minor is under the age of 13 or the age of majority, as determined by the local jurisdiction, and requests the ability to administer their own account (which would require an email for password recovery) then legal notice and opt out parent consent process must be initiated and the credential must carry a Minor Child attribute. The process allows for the collection of a parent online identifier /email in order to inform the Minor Child asserted parent of the credential establishment and use with an option to decline. A parent could choose to initiate a parent self-asserted account credential by taking an affirmative action from the email notice. If affirmative action is not taken to decline the Minor Child credential or establish a
parent credential the Minor Child credential may still be used to log-in, but the Minor Child’s access to content or services requiring affirmative parental consent will be prevented.

If the Minor Teen between the ages of 13 and 17 needs to present proof of their Minor age, then a Parent Verified Credential holder can vouch for the Minor Teen’s age. The Minor Credential will carry a Minor Teen attribute. Other methods of verifying the Minor Teen’s age maybe appropriate.

If an RP requires parental consent for accessing content or services past the age of 13, it shall provide such notice both on its service, sites and to the CMA.

3.2.7 The MTF Institutional Credential

The MTF addresses instances where a Minor’s teacher, scout master, or karate instructor may wish to provide consent for the Minor to access an MTF online service that falls out of the protections afforded by COPPA to educational institutions; however, seeking parental pre-approval for each instance may be impractical. The MTF Institutional Credential enables the Institutional Adult holder to grant consent to access online services that are also MTF RPs on behalf of the Parent. Credential types are determined by the strength of the relationship between the credential holder and the institution they represent and the relationship between the Minor and the credential holder. For example:

- **Educational Self-Asserted Credential** – This credential is available for accredited educational staff. This requires that the self-asserted Educator role is REASONABLY verified and the relationship between the Minor and Educator is REASONABLY established. This credential requires verification of adult status utilizing one of the methods described in 3.2.2. In order to provide consent using an MTF Educational Institutional Credential, the educator must obtain parental consent where the activities and the associated collection or disclosure of Minor’s personal information will extend beyond school-related activities. The MTF adds additional requirements that Educators be given the ability to receive notice, the ability to pre-consent a Child’s access to an educational service, as well as the ability to opt-out.

- **Educational Verified Credential** – This credential is available for accredited educational institutions and their staff. The MTF adds additional requirements that Educators be given the ability to receive notice, the ability to pre-consent a Child’s access to a service, as well as the ability to opt-out. This IAP requires the IdP to verify the applicants’ status as an accredited educator with the appropriate Government educational authorities or with an accredited institution of Higher Education. The school or institution must register as an entity with the CSP or Foundation, and indicate which Educators are authorized to obtain credentials. In order to provide consent using an MTF Educational Institutional Credential, the educator must obtain parental consent where the activities and the associated collection or disclosure of Minor’s personal information will extend beyond school-related activities.

- **Noncommercial organizations** – This credential enables an accredited and authorized member of a non-educational institution (e.g., Boy & Girl Scouts, 4H, Pop Warner Football, places of worship, libraries, etc.), to grant consent to access online services that are also MTF RPs on behalf of the parent. The MTF adds additional requirements that Adults be given the ability to receive notice, the ability to pre-consent

---

4 The FTC recognizes schools’ ability to act in the stead of parents in order to provide in-school Internet access. However, where the activities and the associated collection or disclosure of Children’s personal information will extend beyond school-related activities, the FTC recommends that schools should, as a best practice, effectively notify parents of its intent to allow Children to participate in such online activities before giving consent on parents’ behalf.
a Minor Child’s access to a service, as well as the ability to opt-out. The non-educational institution must register as an entity with the CSP or Foundation, submit to an assessment process as outlined in the FOPP, and indicate which staff are authorized to obtain credentials. This rule requires the IdP to verify the applicants’ status as an authorized Institutional Adult associated with the non-educational institution. In order to provide consent using an MTF NPO Institutional Credential, the Institutional Adult must obtain parental consent where the activities and the associated collection or disclosure of Children’s personal information will extend beyond the NPO related activities. CMAs and/or RPs will remain responsible for notifying the Parent when consent is granted, provide access to information collected, and disclose all relevant privacy policies to both the Parent/Guardian and the Institutional Adult.

3.2 MTF Participant’s Federation Registration and Credential Issuance Process

The following is an overview of the registration and credential issuance process under the MTF. A comprehensive list of roles and requirements follow in this document.

Registration (RP, CSP)
Attribute Proofing (IdP, AA)
Adult Verification (IdP, AA)
Relationship Verification (IdP, AA, CMA)
Credential Issuance (CSP, RP)

Minors and adults may register directly with a CSP or through MTF-supporting RPs. Verified Institutional Adults must register respectively through their accredited educational institution or non-educational institution.

Depending upon which type of MTF Credential is being acquired, information captured at registration is limited to:
- Child or Parent registration information limited and/or collection ordered by regulation.
- Identity proofing of Adult as defined in a non-exhaustive list of methodologies reasonable in the light of available technology as interpreted under COPPA or other jurisdictional regulations.
- Authorized User consented to TOS/EULA.
- Authorized mobile phone number collected from an adult for out-of-band SMS authentication.
- Information captured once and stored in CSP registration database and CMA database for use by many RPs, mitigating the risk of unauthorized access, compromise, and disclosure.

Attribute Proofing

At registration, initial attributes are self-asserted. AAs may proof attributes through their inspection of identity source documents issued by government agencies or others, such as corporations, associations, or other organizations. AAs may in selected cases distribute pre-approved credentials (e.g., for AA company employees) or register Parents or Educators on behalf of the CSP. The CSP may separately verify identity through an IdP depending on the requirements of the CSP, CMA, or RP.
### Attributes Table

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Proofing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor first name, birth date, email</td>
<td>Child or Parent asserted</td>
</tr>
<tr>
<td>Parent first name, online identifier</td>
<td>Child or Parent asserted</td>
</tr>
<tr>
<td>Parent name, email and address (location), DOB, other attributes</td>
<td>Parent asserted</td>
</tr>
<tr>
<td>Parent/Institutional Adult identity</td>
<td>Self asserted, verified by IdP or AA</td>
</tr>
</tbody>
</table>

---

**Adult Verification**

To establish that a person is likely to be an Adult, attributes may be verified by trusted third parties (MTF certified IdPs and AAs). The specific identifier data remains with the IdP or AA, but the information type used for verification is recorded within the CSP’s registration database, such as:

- Self-assertion
- Credit card authorization
- Driver’s licence number
- Last four digits of SSN
- Mobile and cable records
- Public or school records

CSPs will not generally retain any personal identifiers that are considered sensitive such as Social Security numbers (SSN) or financial identifiers such as credit card numbers. Under separate agreements CSPs may be requested to obtain Adult/Minor SSN or equivalent for tax reporting, financial services, and other government or regulated specified uses.

### Relationship Verification

Attributes verified by trusted third parties to authenticate a Parent’s identity may verify a relationship to their associated Minor. Specific identifier data remains with the IdP/AA, but the information type used for verification is recorded within the CSP’s registration database, such as:

- Self-assertion
- Mobile and cable records
- Telephone records
- Public or school records
- Health records
- Birth certificate
- Social Security Administration information
- Federal/State/Local government records including tax filings
- Affiliation with an Association (i.e. Girl Scouts)

### Credential Issuance

CSPs act as the custodian of attribute information and, as such, maintain a registration service of Parents and Minors that serve as the identity store to issue a token or MTF Parent and Minor’s Credential. This credential is used to gain access to the services, applications and information resources required by the access control systems of RPs. MTF credentials may be associated by Users, CSPs, CMAs, or RPs to non-MTF credentials to be used as proxies (i.e., Google ID). An RP’s credential may be associated with a CSPs credential. Some RPs may issue their own credentials, however they are usable only within the online services controlled by the RP.
### 3.3 MTF Participant’s Credential Attributes & Exchange Process

In order to use Federation-compliant authentication credentials, RPs may export or exchange a subset of their registration information with the CSP to provide independent Adult and relationship verification. Any additional data collected, exchanged, and used in conjunction with an MTF Credential must be handled in a transparent manner consistent with the MTF and if linked to a Minor Child account will be treated as PII.

Within the Federation, the basic set of attributes available to be exchanged among RPs by CSPs may include those in the following chart. Any attributes not listed below that are relevant to the RP lay outside of the MTF and requires additional Adult notice and consent to authorize collection and exchange when dealing with a Minor Child.

<table>
<thead>
<tr>
<th>Data Elements</th>
<th>Child (U13)</th>
<th>Minor (13-17)</th>
<th>Adult</th>
<th>Educator/Non-Parent Adult</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth Date/Range</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Unique Identifier (Site Based)</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Password/Pin</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Email</td>
<td>Permitted*</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>First Name</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Last Name</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Gender</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Allowed</td>
<td>Permitted</td>
</tr>
<tr>
<td>Physical Address</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>GPS Location</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>Secret Q&amp;A</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>Device ID</td>
<td>Permitted*</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>Authentication Source</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>MTF Permissions</td>
<td>N/A</td>
<td>Permitted</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>EULA/ToS Acceptance</td>
<td>N/A</td>
<td>Permitted</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Trusted Institutional Parties</td>
<td>N/A</td>
<td>Permitted</td>
<td>Permitted</td>
<td>Required</td>
</tr>
</tbody>
</table>

*Permitted with Parental Consent
### 3.4 MTF Participant’s Credential Authentication Process

Credentials are authorized using industry standard mechanisms such as OpenID Connect or SAML.

### 4 Minors Trust Framework: Operating Processes

#### 4.1 MTF Roles and Prerequisites

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relying Party (RP)</strong></td>
<td>Online services, merchants, communications carriers, application developers, media companies, and others who agree to accept MTF Credentials. Consumes MTF Credentials and enables CMA operation.</td>
<td>Must be COPPA-certified. May only use pseudonyms, nicknames, device IDs, or email addresses as User IDs. Must prohibit the use of real names in a public facing setting as display name unless express Adult consent is obtained.</td>
</tr>
<tr>
<td><strong>Credential Service Provider (CSP)</strong></td>
<td>Delivers registration, verification, compliance and information services for issuance and acceptance of MTF Credential by Federation Members.</td>
<td>Must deliver unique, interoperable pseudonymous identifiers to interact with RPs and other Federation Members.</td>
</tr>
<tr>
<td><strong>Consent Management Authority (CMA)</strong></td>
<td>Manages consent by Parents, Delegated Adults or Institutional Adults for Child/Teen use of RP services, features, and functions.</td>
<td>Must provide tools to manage multiple consents, notifications, and associations.</td>
</tr>
<tr>
<td><strong>Identity Provider (IdP)</strong></td>
<td>Verifies and/or authenticates identities by determining an asserted User is who they say they are. IdPs include credit reporting agencies, banks, health services, employers, public record aggregators, government agencies and others. May also act as an AA.</td>
<td>Allow verification and/or authentication of MTF Credential holders, including association to the Child/Teen.</td>
</tr>
<tr>
<td><strong>Attribute Authority (AA)</strong></td>
<td>Verifies any number of personal or relationship attributes needed for the MTF Credential. May include Federal, State, or local governments, schools, service and commercial organizations, or technology service providers who may verify unique device characteristics.</td>
<td>Must assist in the verification and/or authentication of MTF Credential holders, including association to the Minor, and association to other organizations.</td>
</tr>
<tr>
<td><strong>Assessor</strong></td>
<td>Determines whether MTF participants are in contractual compliance as set forth by the MTF. Key areas include how PII is collected, publicly disclosed, used, managed, exchanged, transmitted, transferred,</td>
<td>Must have current direct experience as an information assurance assessor and perform assessments regularly in a professional capacity. Demonstrated qualification, such as designation as a</td>
</tr>
</tbody>
</table>
17 | P a g e

| Dispute Resolution Service Provider (DRSP) | Provides an effective redress mechanism for individuals who feel their personal information, or that of their Child or Teen, may have been misused or disclosed with unauthorized parties. | Must be an independent third-party. Process is based on FTC COPPA Safe Harbor Dispute Resolution process. Members who are FTC COPPA Safe Harbors may provide DSRP services. |

### 4.2 MTF REQUIREMENTS: ALL PARTICIPANTS

#### 4.2.1 DATA POLICY

- **Data Collection:** User access cannot be conditioned on collecting more information than is reasonably necessary to deliver service or functionality requested.
- **Data Sharing:** Onward transfer of Child, Teen, or Parent collected information is prohibited without User or Parental consent. Federation participants shall not collect, store, use, process, or share other Child PII, as defined by COPPA, without Parental consent. Federation Participants shall prevent 3rd parties from overtly or surreptitiously collecting Minor PII without User or Parental consent.
- **Data Storage:** Personally identifiable information may not be retained longer than time necessary for providing and administering the services for which the information was collected, except otherwise as required by law.
- **Data Alteration, Deletion & Destruction:** Users are entitled to access and make choices regarding their data use, or data of related Child/Teen. Choices shall be automatically transmitted and applied to all applicable parties with whom that User or Child/Teen interacts. Timely elimination of data is the ultimate protection against misuse or unauthorized disclosure; as such any information being eliminated must be securely destroyed per NIST SP 800-88, Guidelines for Media Sanitization.
- **Secure Data Transmission:** All participants within the Federation agree to use current proven best practices to secure data when transmitting PII.
- **Data Rights:** The information associated with the individual Federation-approved credential and the credential itself may not be used for commercial purposes without Adult consent for Children under 13. All information shall be protected, transferred at the User’s request, and securely destroyed when terminating business operations per NIST SP 800-88, Guidelines for Media Sanitization.

#### 4.2.2 LINKING OR ASSOCIATING POLICY

Linking of any Child’s personal information derived from a credential or its use for any purposes beyond that of providing service delivery, customer service, or for other operational purposes is prohibited without consent from a Parent.

#### 4.2.3 SECURITY REQUIREMENTS

Federation Participants must adhere to industry standard best practices for safely handling personally identifiable information, attributes, and general information. These practices require that organizational control measures are in place, such as security policies, procedures and processes, and that employees involved in the processes are adequately trained.
4.2.4 **Permissions or Authorization Policy**

All participants within the MTF agree to abide to all applicable laws and related rules dealing with Children’s personal information, as required by both their applicable domestic and foreign law.

4.2.5 **Breach Notification Policy**

- **In General:** A breach incident is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the Federation Participant. Breaches shall include unconsented overt disclosure of PII by a Child (i.e. disclosing home address in a chat). Federation Participants are required to notify the Foundation immediately upon knowledge of a breach incident, as well as to comply with all legal requirements. Federation Participants will have mechanisms and processes in place to notify Users if their unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person. The breach disclosure shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the integrity of supporting information systems.

- **Good-Faith Acquisition:** Good-faith acquisition of PII by an employee or agent of the Federation Participant on behalf of the Organization is not a breach of the security of the system, provided that the PII is not used or subject to further use or unauthorized disclosure.

- **Third-Party Data Notification:** A third-party contractor to a Federation Participant that maintains computerized data that includes PII that the Participant does not own, must notify the Foundation of any breach of the security of the data following discovery if the PII was, or is reasonably believed to have been, acquired by an unauthorized person. Notice must be provided in written or electronic form where permitted to all affected parties.

- **Notice Requirements:** The notice shall be clear and conspicuous and shall include a description of the following: Date of the notice; Name and contact information for the Federation Participant; Type of PII subject to the unauthorized access and acquisition; the date, estimated date, or date range during which the breach occurred, if it can be determined; Whether notification was delayed as a result of law enforcement investigation, if that can be determined; A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and Information about what the Participant has done to protect individuals whose information has been breached.

4.2.6 **Designated Purpose Policy**

MTF Federation compliant systems capture, integrate, and exchange information for the purpose of issuing electronic credentials to Children, Teens, and related Adults; and simplifying the process of obtaining verifiable Parental consent. MTF Federation compliant systems may collect other data used in the normal course of service for internal non-marketing use only, without obtaining Parental notice and consent. Other data may include cookies, non-fine grained location data, and similar items permitted by COPPA.

4.2.7 **Privacy Policy**

All Federation Participants shall publish a privacy policy describing what User-identifying information is captured, how used, and under what conditions it may be released consistent with the Federation. Under COPPA privacy notices are required in conjunction with transactions that request to collect, use or disclose PII of Users.
4.2.8 CONFIDENTIALITY POLICY

All Federation Participants will maintain confidentiality of registration and usage information through enforcing technology and agreements, where applicable.

4.2.9 COMPLIANCE POLICY

Organizations that adopt, implement, and enforce Federation provisions may signify their acceptance through a digital seal issued by the CSP Member, prominently displayed on their domain. The Foundation will detail the digital seal requirements. The MTF requires all Participants to comply with applicable state and federal regulation concerning protection of PII, as well as all applicable laws and related rules dealing with Child personal information, as required by both their applicable domestic and foreign law.

4.2.10 DATA MONETIZATION POLICY

The information associated with the individual Federation-approved credential and the credential itself may not be used for commercial purposes without explicit User or parental consent for Children under 13.

4.3 MTF ROLE-BASED REQUIREMENTS: RELYING PARTIES

These requirements are in addition to those imposed upon all Federation Participants.

4.3.1 RP DESCRIPTION AND GENERAL REQUIREMENTS

RPs are online services, merchants, communications carriers, application developers, media companies, and others who agree to accept MTF Credentials. RPs consume MTF Credentials and enable CMA operation. RPs may also create their own MTF Credentials, but for use only in properties controlled by the RP. RPs are required to be COPPA-certified through self-certification or 3rd party assessment and certification by authorized organizations.

4.3.2 RP IDENTIFIER POLICY

In general, CSPs are responsible for the User ID; RPs will also be responsible if they maintain their own log-in procedures. CSPs and RPs may only use pseudonyms, nicknames, device IDs, or email addresses as user IDs to reduce the risk of Child identification, and shall prohibit the use of real names or other PII in a public facing setting as display names. Verification will be done by cross-checking the user ID/display name against Child's name if provided during registration. Parents must be shown their Child user ID/display name to ensure real names or other PII is not used in public display. RPs should encourage credential holders to have unique display names at all sites.

4.3.3 RP DATA POLICY

- Initial COPPA registration: During the initial registration, COPPA limits RP data collection to: Child First Name, DOB, Primary Adult email or other online identifier.
- Post-COPPA registration MTF enrollment: RPs may collect a Child's MTF credential and Child's screen name, in addition to any information expressly authorized by Parent. Federation RPs agree to minimize the capture and retention of registration information beyond the MTF Child's Credential. Child PII may not be shared without Adult consent. RPs agree to link their registration and authentication processes for Children with the CSP if a related Parent account is held separately with the CSP of the Parent. RPs may collect additional attributes with parental consent. Non-PII attributes, such as the creation of an
avatar or likes and dislikes, do not require parental consent. However, when combined PII, these attributes become PII and are protected by COPPA, where sharing requires parental consent.

- **Collection Outside of MTF**: RPs are responsible for the systems, services and applications they make available to MTF Users.
- **Data Sharing**: RPs may only link one specific User with one CSP. If an associated Child’s account is created at a CSP, then the Adult account must also be from the same CSP.
- **Data Rights**: The rights to the information derived from the use of CSP issued credentials within an RP’s domain remain the property of the RP.

### 4.3.4 RP COMMUNICATION RESTRICTIONS & REQUIREMENTS

RPs may only communicate with Credential holders, CSPs, and CMAs. All Internet connections between CSPs and RPs shall be secured with encrypted communications. RPs are responsible for implementing industry-standard secure encrypted communications. RPs are responsible for User interaction with their systems and should protect their systems by taking active measures to detect, deter and defend against unauthorized parties accessing its computing resources for malicious purposes using adequate boundary protection controls.

### 4.3.5 RP TRACKING POLICY

RPs may employ cookies or other identifiers for CSP authentication, tracking, supporting and profiling user activities for the purposes of administration, security and access of their online services within their service for Children without Parental consent. Use of cookies or other identifiers for marketing purposes may only be conducted with explicit parental consent. RPs must obtain Parental consent prior to tracking the Child’s Credential across MTF domains either for themselves or the use of a third-party service, and Adults may revoke that permission at any time.

### 4.3.6 RP PERMISSIONS OR AUTHORIZATION POLICY

Based on defined IAPs, RPs are responsible for establishing access control, authorization, roles, and permissions associated with Users accessing their services and system resources. RPs may use the services of CSPs, CMAs, and AAs to establish the IAP for their Users. RPs are responsible for confirming that display/screen names of Children are not their actual names to the extent possible. RPs must obtain parental consent if displaying the real name or other PII of a Child. CSPs, however, are responsible for confirming the MTF Credential identifiers of Children are not actual names to the extent possible.

### 4.3.7 RP MATERIAL CHANGE/SURVIVABILITY POLICY

When an RP materially changes their policies regarding MTF-approved services, they must notify Parents of Children and Teens, and Institutional Adults, and give them a reasonable amount of time to provide opt-in consent to the new policies. RPs may operate under the old policy or refuse service to the account until the User either grants consent or requests deactivation/deletion.

### 4.3.8 RP CREDENTIAL ISSUANCE

If issuing credentials, RPs shall issue Federation-approved “Basic” credentials free upon request. RPs shall only issue Federation-approved Parent Verified/Parent Verified Plus /Delegated Adult/Institutional Adult credentials upon verification identity. One-time passwords are delivered out-of-band, passwords shall be user-generated, and PIN numbers, if used, shall be either user-generated or delivered out-of-band.

### 4.3.9 CSP NOTIFICATION

RPs agree to notify relevant Federation CSPs within 24 hours if they have reason to believe a credential has been compromised or used inappropriately. Federation CSPs will notify Adults and take corrective action based on the terms of their EULA and/or Terms of Use.
4.3.10 RP Privacy Policy

RPs shall make available their privacy policy and end-user license agreement (EULA) or terms of service (TOS) documents to Parents on their website, within their app, during registration and in a permanent position, and to CMS for publication or linking.

4.3.11 RP MTF Compliance Assessment Policy

MTF compliance may be self-asserted according to Foundation requirements, but will remain subject to random Assessments, the cost of which will be borne by the RP.

4.3.12 RP COPPA Compliance Policy

RPs must be COPPA certified and compliant.

4.3.13 RP Authentication Technologies

MTF members may choose to strengthen authentication and facilitate consent through a range of identifiers, Proof of Knowledge, SMS mobile alert, device identifiers or biometrics beyond what is required by the MTF. Members such as cable carriers may integrate these or MTF User identifiers with existing parental permission systems.

4.3.14 RP User Support Process

Adults who require assistance with the enrollment process, interpreting MTF Children’s Credential usage reports, or modifying attributes and permissions must be allowed to engage RP online or via a customer support help desk for RPs who issue MTF Credentials. Support services will be rendered upon authentication through the secret question retained within the RP’s registration database, by out-of-band SMS authentication via the parent’s mobile phone, or other methods. Frequently asked questions and MTF reference material must be made available through all RP and CSP websites.

4.3.15 RP Dispute Resolution Process

RPs must provide the Parent and the Minor with reasonable and effective means to submit complaints that they may have about the Member’s information practices. All Users may also submit complaints to the Foundation’s Ombudsman. RPs are required to have a representative respond to all complaints immediately. RPs must agree to work with CMA representatives in their efforts to resolve all complaints that are submitted. RPs and the Foundation may utilize the services of a DRSP to resolve User complaints. Disputes between consumers and Federation Participants are discussed at length in the FOPP.

4.4 MTF Role-Based Requirements: Credential Service Providers

These requirements are in addition to those imposed upon all MTF Participants.

4.4.1 CSP Description and General Requirements

CSPs deliver registration, verification, compliance and information services for issuance and acceptance of MTF Credentials by Federation Participants. CSPs must deliver unique pseudonymous identifiers to interoperate and interact with RPs, CMAs, and other MTF-approved CSPs.

4.4.2 CSP Registration Policy

CSPs may obtain registration information from the User or RPs. The CSP retains the registration information necessary to enroll the User. In the case of Children requiring consent, additional information may be collected and retained to contact the Parent, verify Parent identity, and obtain consent. At the time of registration, a second authentication factor may be required that is known only to the User and CSP to support authentication,
COPPA verifiable parental consent, notification and/or customer service activities. Personal information captured by Federation CSPs at registration may only be disclosed to a Relying Party by permission of the Parent and only then when required by EULA/TOS, local laws, or Parent. Personal information may not be retained longer than the time necessary for providing and administering the services for which the information was collected, except as otherwise required by law.

### 4.4.3 CSP Identifier Policy

In general, CSPs are responsible for the User ID; RPs will also be responsible if they maintain their own log-in procedures. CSPs and RPs may only use pseudonyms, nicknames, device IDs, or email addresses as user IDs to reduce the risk of Child/Minor identification, and shall prohibit the use of real names or other PII in a public facing setting as display names. Verification will be done by cross-checking the user ID against Child’s name if provided during registration, and Parents will be shown their Child’s user ID/display name to ensure real names or other PII is not used. CSPs should encourage credential holders to have unique display names at all sites.

### 4.4.4 CSP Data Policy

- **Data Collection**: CSPs may collect registration information from an RP or the User. Information for second-factor authentication known only by CSP and User to support authentication is permitted. Registration data shall be limited to specific purpose unless consent obtained. Required Child/Teen information to be collected: birth date/range; unique user/acct/display name; email (for 13+); password. A CSP may also collect the Child/Teen’s: first/last name; email; gender; and physical/GPS location. The CSP may also collect Adult’s: name; email; date of birth; physical/GPS location; telephone number; site-based UID; gender; password; secret question & answer; device ID; authentication source; MTF permissions; and EULA/TOS acceptance. CSPs are not responsible for any registration processes that request user identification information beyond what is specified by the MTF.
- **Data Sharing**: CSPs may share Child’s information with RP only with permission of User and when required by EULA, TOS, local laws, or Parent. The MTF Credential is only known to the CSP - all other parties receive a pseudonymous value representing the CSP’s credential. The User’s pseudonymous value will be unique to each party to prevent cross-tracing user information across sites.
- **Data Rights**: The rights to the information derived from the compilation, aggregation or cross-domain utilization of CSP issued credentials remain the property of the CSP. CSPs must provide notice in their privacy policies on their policy on the compilation, aggregation, or cross-domain utilization of information derived from CSP-issued Credentials.

### 4.4.5 CSP Communication Requirements & Restrictions

CSPs may communicate with credential holders, RPs, IdPs, AAs, and other CSPs (to determine if a credential has already been issued). All Internet connections between CSPs and RPs shall be secured with encrypted communications.

### 4.4.6 CSP Tracking Policy

CSPs may track identifiers such as the MTF Child’s Credential (unique to each RP) among Relying Party domains and share this information with Parents and to the RPs for features and functions that have been approved by Parents.

### 4.4.7 CSP Security Policy

CSPs must make best efforts to comply with ISO 27000.
4.4.8 CSP CREDENTIAL ISSUANCE POLICY

CSPs shall issue MTF-approved “Basic” credentials free upon request. CSPs shall only issue MTF-approved Parent Verified/Parent Verified Plus/Delegated Adult/Institutional Adult credentials upon verification of identity. One-time passwords are delivered out-of-band, passwords shall be user-generated, and PIN numbers, if used, shall be either user-generated or delivered out-of-band.

4.4.9 CSP CREDENTIAL PROVISIONING

MTF User Credentials are issued electronically by the CSP to Users when requested by a User during the enrollment process. Participating Adults must accept a Participant-issued, Foundation-approved End User License Agreement (EULA) governing the credential.

4.4.10 CREDENTIAL SUSPENSION

CSPs will suspend the use of the User credential within one business day upon notification from an Adult to suspend the credential. CSPs will revoke the Child credential if Adult consent is required and is not obtained within 5 business days.

4.4.11 CSP NOTIFICATION

RPs agree to notify relevant Federation CSPs within 24 hours if they have reason to believe a credential has been compromised or used inappropriately. Federation CSPs will notify Adults and take corrective action based on the terms of their EULA and/or Terms of Use.

4.4.12 CSP AUTHENTICATION TECHNOLOGIES

Federation Participants may choose to strengthen authentication and facilitate consent through a range of identifiers, Proof of Knowledge, SMS mobile alert, device identifiers or biometrics beyond what is required by the MTF. Participants such as cable or mobile carriers may integrate these or MTF User identifiers with existing parental permission systems.

4.4.13 CSP ASSERTIONS AND CREDENTIALS

In order to extend single sign on to users accessing RPs web based applications, CSPs will send identity attribute assertions based upon the Security Assertion Markup Language (SAML) or other standards-based credential conventions (e.g., OpenID Connect). CSPs will support two-factor authentication but two-factor authentication shall not be required for system access.

4.4.14 CSP INFRASTRUCTURE

CSP’s will operate their service within a SAS70 Type II certified operating environment.

4.4.15 CSP RECORDS RETENTION POLICY

In addition to the requirements under COPPA, CSPs shall retain active registration and usage records of individual users no longer than one month following notification of the choice to discontinue the MTF Child's Credential. This does not apply to backup data, however, if recovered, the data will be deleted.

4.4.16 CSP RECORDS INSPECTION POLICY

Parents and Teens (13+) will have on-demand access to all User-provided information and Federation credential records, and the records specific to their associated Child, including where the credential has been linked to. Upon authentication, Adults, Parents and Minors may view, request deletion or correction of attribute information, or discontinue the use of a CSP for their Child or themselves. They may also choose to restrict or change the RPs and related features and functions that the Child may access or exchange PII with. Due to COPPA
requirements, any changes in email addresses or other verified data must be re-verified. Self-asserted information will not be verified.

4.4.17 CSP Log Files

CSPs will make available to the Foundation and law enforcement, government officials, or other third parties pursuant to a subpoena, court order, or other legal process or requirement applicable to the CSP log files with audit trails describing specific interactions between a User and a requesting RP.

4.4.18 CSP User Support Process

Adults who require assistance with the enrollment process, interpreting MTF Child’s Credential usage reports, or modifying attributes and permissions must be allowed to engage RP online or via a customer support help desk. Support services will be rendered upon authentication through the secret question retained within the RP’s registration database, by out-of-band SMS authentication via the parent’s mobile phone, or other methods. Frequently asked questions and MTF reference material must be made available through all RP and CSP websites. Parents may revoke either their own Parent credential or the credential of a Child/Teen for whom they are responsible at any time by notifying the CSP. The CSP will notify RPs of the revocation within 30 days of parental notification.

4.4.19 CSP Business Continuity

CSPs agree to implement recovery procedures and systems necessary to maintain operation and avoid an extended outage greater than four (4) hours per month. CSPs will conclude Service Level Agreements (SLAs) with system infrastructure providers to support high availability.

4.4.20 CSP Compliance Assessment Policy

CSPs will submit to an annual assessment of its policies, practices, and processes by an independent third-party Assessor.

4.4.21 CSP Compliance Policy

The MTF requires CSPs to ensure compliance with the provisions of COPPA and FERPA and create the supporting policies, agreements, processes and systems to warrant COPPA compliance of RPs. Enforcement of COPPA and its provisions is the sole jurisdiction of the Federal Trade Commission and the States.

4.4.22 CSP Data Monetization Policy

The commercial rights to the de-identified information derived from the compilation or aggregation of issued credentials remain the property of the CSP. CSPs receive a perpetual royalty free license to aggregate, analyze and publish anonymous audience level information to RPs, regulators and others at its sole discretion.

4.4.23 Dispute Resolution Process

CSPs will assist a parent to contact an RP or CMA whenever they feel information about themselves or their Child/Teen or their consent has been inappropriately disclosed.

4.4.24 Insurance

CSPs shall maintain errors and omissions insurance coverage for operations including issuance of credentials and any misidentification that may result from failures to follow the processes described in the MTF.

4.5 MTF Role-Based Requirements: Consent Management Authorities

These requirements are in addition to those imposed upon all Federation Participants.
4.5.1 CMA Description and General Requirements

CMAs manage consent by Parents, Delegated Adults, and Institutional Adults for Child/Teen use of RP services, features, and functions. CMAs must provide tools to manage multiple consents, notifications, and associations. CMAs will update their RP directory on a regular basis from a master directory of all RPs in good standing, to be maintained by the Foundation.

CMAs must provide Parents the opportunity to consent to all MTF-approved destinations and their features and/or functions with which their Children/Teens authenticate themselves based on COPPA requirements, service-determined age requirements, or service-determined site functionality.

CMAs must give Parents the ability to pre-grant consent for an RP within the MTF with a CMA and/or choose to be notified whenever their Child/Teen’s credential is requesting consent to access new or previously unapproved MTF RPs, their features and/or functions.

Parents must be allowed to deny Child/Teen access to online services and their features and/or functions at their discretion based on previous consent.

4.5.2 CMA Data Policy

- **Data Collection:** CMAs may only collect Child, Designated Adult, and Institutional Adult MTF credential attributes associated to the actual authorization processed.
- **Data Alteration, Deletion & Destruction:** CMAs must establish reasonable procedures for the destruction of PII once it is no longer necessary for the fulfillment of the purpose for which it was collected, or at the User’s request. Must establish procedures for the proper disposal of electronic media containing sensitive data as required by COPPA or other applicable law.

4.5.3 CMA Communication Restrictions

CMAs may communicate with adult credential holders and RPs.

4.5.4 CMA Security Requirements

CMAs must make best efforts to comply with ISO 27000.

4.5.5 CMA Authentication Technologies

Federation Participants may choose to strengthen authentication and facilitate consent through a range of identifiers, Proof of Knowledge, SMS mobile alert, device identifiers or biometrics beyond what is required by the MTF. Members such as cable carriers may integrate these or MTF User identifiers with existing parental permission systems.

4.5.6 CMA Compliance Assessment Policy

Compliance may be self-asserted according to Foundation requirements, but will remain subject to random Assessments, the cost of which is to be borne by the CMA.

4.5.7 CMA Compliance Policy

The MTF requires CMAs to ensure compliance with the provisions of COPPA and FERPA and create the supporting policies, agreements, processes and systems to warrant COPPA compliance of RPs. Enforcement of COPPA provisions is the sole jurisdiction of the Federal Trade Commission and the States.
4.5.8 **CMA Data Monetization Policy**

The commercial rights to the de-identified information derived from the compilation or aggregation of issued credentials remain the property of the CMA. CMAs receive a perpetual royalty free license to aggregate, analyze and publish anonymous audience level information to RPs, regulators and others at its sole discretion.

4.5.9 **CMA Dispute Resolution Process**

CMAs must provide the Parent and the Child with reasonable and effective means to submit complaints that they may have about the Member’s information practices. MTF Credential users may also submit complaints to the Foundation’s Ombudsman. CMAs are required to have a representative respond to all complaints immediately. CMAs must agree to work with RP representatives in their efforts to resolve all complaints that are submitted. CMAs and The Foundation may utilize the services of a DRSP to resolve User complaints. Disputes between consumers and Federation Participants are discussed at length in the FOPP.

4.6 **MTF Role-Based Requirements: Identity Providers**

These requirements are in addition to those imposed upon all MTF Participants.

4.6.1 **IdP Description and General Requirements**

IdPs may be credit reporting agencies, banks, health services, employers, public record aggregators, government agencies and others who verify and/or authenticate identities by determining an asserted User is who they say they are. They may also act as an AA. IdPs allow verification and/or authentication of MTF Credential holders, including association to the Minor.

4.6.2 **IdP Data Policy**

- **Data Collection**: IdPs may collect employment verification, age of Adult, legal name, date of birth, email address, street address, minor dependents, relationship to minors, affiliations, and parental consent.
- **Data Sharing**: IdPs may only forward attribute information and known user associations to a CSP.

4.6.3 **IdP Communication Restrictions:**

IdPs may only communicate with CSPs.

4.6.4 **IdP Security Requirements**

IdPs must make best efforts to comply with ISO 27000.

4.6.5 **IdP Compliance Assessment Policy**

Compliance may be self-asserted according to Foundation requirements, but will remain subject to random Assessments, the cost of which will be borne by the IdP.

4.6.6 **IdP Insurance**

IdPs shall maintain errors and omissions insurance coverage for operations including issuance of credentials and any misidentification that may results from failures to follow the processes described in the MTF.

4.7 **MTF Role-Based Requirements: Attribute Authorities**

These requirements are in addition to those imposed upon all Federation Participants.
4.7.1 AA DESCRIPTION AND GENERAL REQUIREMENTS
AAs verify any number of personal or relationship attributes needed for the MTF Credential. AAs may include Federal, State, or local governments, schools, service and commercial organizations, or technology organizations who may verify unique device characteristics. AAs must assist in the verification and/or authentication of MTF Credential holders, including association to the Child, and association to other organizations.

4.7.2 AA DATA POLICY
- Data Collection: AAs may collect employment verification, age of Adult, legal name, date of birth, email address, street address, minor dependents, relationship to minors, affiliations, parental consent.
- Data Sharing: AAs may only forward attribute information and known user associations to a CSP.

4.7.3 AA COMMUNICATION RESTRICTIONS
AAs may only communicate with CSPs and IdPs.

4.7.4 AA SECURITY REQUIREMENTS
AAs must make best efforts to comply with ISO 27000.

4.7.5 AA COMPLIANCE ASSESSMENT POLICY
Compliance may be self-asserted according to Foundation requirements, but will remain subject to random Assessments, the cost of which will be borne by the AA.

4.8 MTF ROLE-BASED REQUIREMENTS: ASSESSORS
These requirements are in addition to those imposed upon all Federation Participants.

4.8.1 ASSESSOR DESCRIPTION AND GENERAL REQUIREMENTS
Assessors determine whether Federation Participants are in contractual compliance as set forth by the MTF. Key areas include how PII is collected, publicly disclosed, used, managed, exchanged, transmitted, transferred, retained, and destroyed. Adherence to an organization’s published privacy policy and Federation requirements are also assessed, as well as its practices and representations. Assessors must have current direct experience as an information assurance assessor and perform assessments regularly in a professional capacity. Demonstrated qualification, such as designation as a Certified Information System Auditor (CISA), and FTC-approved COPPA Safe Harbor or equivalent knowledge and experience is required.

Assessors will oversee MTF compliance by CSPs, IdPs, CMAs, RPs and AAs. Auditors may randomly sample CSPs, IdPs, RPs and AAs including but not limited to those who self-assert compliance. The costs will be borne by those being assessed.

The Assessor is an external party and member in good standing with the GTA. The Assessor conducting the review must be objective and independent, following guidelines established by professional assessment and audit organizations, such as The Institute of Internal Auditors “Standards for the Professional Practice of Internal Auditing”.5

5 http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/
The Assessor shall possess adequate technical proficiency and industry knowledge for the specific assessment being performed, as put forth in the Assessor Requirements. The Assessor must have demonstrated qualification to make competent determination of the Federation Participant’s compliance with applicable criteria, taking into account technical issues and specific requirements that the criteria might set out (e.g., specific management processes) as determined by the Foundation. The Assessor shall have, as a minimum:

- Understanding of the Federation Participant’s industry and services;
- General knowledge of the business process being assessed;
- Technical awareness and management audit experience;
- Familiarity with applicable regulation (i.e., COPPA or FERPA requirements); and
- Understanding of the provisions of the MTF.

To review a Federation Participant, the Assessor must have current direct experience as an information assurance assessor and perform assessments regularly in a professional capacity. Demonstrated qualification, such as designation as a Certified Information System Auditor (CISA)\(^6\), an FTC approved COPPA Safe Harbor or equivalent knowledge and experience, is required. Additional, specific requirements for Assessors will be developed by the Foundation.

### 4.9 MTF ROLE-BASED REQUIREMENTS: DISPUTE RESOLUTION SERVICE PROVIDERS

These requirements are in addition to those imposed upon all Federation Participants.

#### 4.9.1 DRSP DESCRIPTION AND GENERAL REQUIREMENTS

DRSPs provide an effective redress mechanism for individuals who feel their personal information, or that of their Child or Minor, may have been misused or disclosed with unauthorized parties. DRSPs must be an independent third-party. The DRSP process is based on FTC COPPA Safe Harbor Dispute Resolution process, See 16 C.F.R § 312.11. Members who are FTC COPPA Safe Harbors may provide DRSP services. An organization acting as an Assessor may not provide DRSP services for an MTF Participant they have assessed. The DRSP will produce and submit to the Foundation a report of every action handled, whether the individual complaining has had the matter resolved to their satisfaction, and if needed, its recommendation for additional action or redress by the Foundation.

\(^6\) See Information Systems Audit and Control Association http://www.isaca.org/
4.10 MTF FUNCTIONAL ELEMENTS

The functional elements — basic operations that may occur in online identity-related interactions — are grouped into core operations. Not all elements will be invoked in every identity interaction, and some may be invoked multiple times. While logically some functions are likely to occur before or after others, there is no explicit order specified in the model.

4.10.1 FUNCTIONAL ELEMENTS DIAGRAM

To improve readability, the functional elements layer is presented in a single diagram including all functional elements and core operations.
## 4.10.2 Functional Elements Description Matrix

The functional elements description matrix provides brief descriptions of each core operation and functional element. MTF functional requirements are found in Section 4.11.

<table>
<thead>
<tr>
<th>Core Operation</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>Process that establishes a digital identity for the purpose of issuing or associating a credential.</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Process by which an entity or agent requests initiation of registration.</td>
<td></td>
</tr>
<tr>
<td>Attribute Control</td>
<td>Process of managing and releasing attributes for the purposes of registration or authorization.</td>
<td></td>
</tr>
<tr>
<td>Attribute Verification</td>
<td>Process of confirming or denying that claimed identity attributes are correct and meet the pre-determined requirements for accuracy, assurance, etc.</td>
<td></td>
</tr>
<tr>
<td>Eligibility Decision</td>
<td>Decision that an entity does or does not meet the pre-determined eligibility requirements for a digital identity or credential.</td>
<td></td>
</tr>
<tr>
<td>Credentialing</td>
<td>Process to bind an established digital identity with a credential.</td>
<td></td>
</tr>
<tr>
<td>Credential Provisioning</td>
<td>Process by which ownership of a credential is conferred, confirmed, or associated with a digital identity.</td>
<td></td>
</tr>
<tr>
<td>Token Binding</td>
<td>Process of binding a physical or electronic token to a credential.</td>
<td></td>
</tr>
<tr>
<td>Attribute Binding</td>
<td>Process of binding attributes to a credential.</td>
<td></td>
</tr>
<tr>
<td>Revocation</td>
<td>Process by which an issuing authority renders a digital identity, issued credential, token, or verified attribute invalid for authentication or authorization.</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Process of determining the validity of one or more credentials used to claim a digital identity.</td>
<td></td>
</tr>
<tr>
<td>Authentication Request</td>
<td>Process by which authentication is initiated by an entity.</td>
<td></td>
</tr>
<tr>
<td>Credential Presentation</td>
<td>Process by which an entity submits a credential for the purposes of authentication.</td>
<td></td>
</tr>
<tr>
<td>Credential Validation</td>
<td>Process of establishing the validity of the presented credential.</td>
<td></td>
</tr>
<tr>
<td>Authentication Decision</td>
<td>Decision to accept or not accept the results of the credential validation process.</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td>Process of granting or denying specific requests for access to resources.</td>
<td></td>
</tr>
<tr>
<td>Authorization Request</td>
<td>Process by which authorization is initiated by an entity.</td>
<td></td>
</tr>
<tr>
<td>Core Operation</td>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Attribute Control</td>
<td>Process of managing and releasing attributes for the purposes of registration or authorization.</td>
<td></td>
</tr>
<tr>
<td>Attribute Verification</td>
<td>Process of confirming or denying that claimed attributes are correct and meet the pre-determined requirements for authorization; typically, these attributes for authorization have not been bound to the credential or previously available to the organization making the authorization decision.</td>
<td></td>
</tr>
<tr>
<td>Authorization Decision</td>
<td>Decision to grant and deny access to a resource based on the results of the authorization processes and policies.</td>
<td></td>
</tr>
<tr>
<td>Transaction Intermediation</td>
<td>Processes and procedures that limit linkages between transactions and facilitate credential portability.</td>
<td></td>
</tr>
<tr>
<td>Blinding</td>
<td>Process by which service providers involved in a transaction are prevented from observing each other (i.e., a relying party does not know which credential service provider an entity is utilizing in a transaction or vice versa). Based upon the transaction type and the number of service providers involved, blinding may be done to prevent a single, multiple, or all service providers from viewing the other participating services.</td>
<td></td>
</tr>
<tr>
<td>Pseudonymization/Anonymization</td>
<td>Process by which an intermediary prevents service providers from linking a digital identity with a particular person or entity.</td>
<td></td>
</tr>
<tr>
<td>Exchange</td>
<td>Process by which one protocol is translated to another for consumption by different entities involved in a transaction.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.10.3 Functional Roles Description Matrix

This table provides descriptions of the roles in the functional elements layer. These are intended to provide Federation Participants with a common understanding of the functions typically executed by the identified roles. Note that a Federation participant may serve more than one role and serving a role does not require the participant to execute all of the functions in that role. Additionally, this list is not intended to restrict organizations from executing any of the ecosystem functions. MTF functional requirements are found in Section 4.11.

<table>
<thead>
<tr>
<th>Role</th>
<th>Registration</th>
<th>Credentialing</th>
<th>Authentication Request</th>
<th>Authorization</th>
<th>Transaction Intermediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Person attempting to establish a digital identity and/or use a credential to access a protected resource</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Credential Service Provider (CSP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manages the credentialing and authentication core operations</td>
<td>● ● ● ●</td>
<td>● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent Management Authority (CMA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manages consents by Parents/Guardians, Educators, or other Authorized Adults for Child/Minor use of RP services, features, and functions</td>
<td>● ● ●</td>
<td>● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Service Provider</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Manages authentication core operations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Authority (RA)</td>
<td></td>
<td></td>
<td></td>
<td>● ● ●</td>
<td></td>
</tr>
<tr>
<td>Manages the registration core operation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Provider (IDP)</td>
<td></td>
<td></td>
<td></td>
<td>● ● ● ●</td>
<td></td>
</tr>
<tr>
<td>Manages the registration, credentialing, and authentication core operation.</td>
<td>● ● ● ●</td>
<td>● ● ● ●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute Authority (AA)</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Executes the attribute verification and attribute control functions in support of the core operations. May include Federal, State, or local governments, schools, service and commercial organizations, or technology organizations who may verify unique device characteristics.</td>
<td>●</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Relying Party (RP)</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Relies upon other entities to execute the core operations and functions in order to authorize access to protected resources.</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intermediary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>● ● ●</td>
</tr>
<tr>
<td>Executes the transaction intermediary core operation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5 CERTIFICATION REQUIREMENTS

5.1 MTF Certification Requirements: All Participants
The certification processes are maintained by the Foundation as part of its governance and operating structure. These criteria set the requirements for MTF participants. These criteria focus on business and technical conformity of MTF participants to the MTF requirements as a means to establish trust throughout the MTF. The assessment criteria focus on three main areas: organizational, business and technical requirements as described in this section.

5.2 Certification Process

5.3 Certification Criteria
The following sections identify the criteria by which MTF participants will be certified.

5.4 Prior Certification
The following certification processes are recognized under the Framework: OIX, Kantara, Safe BioPharma. The certification documents are separate documents and made part of the MTF.

5.5 Organizational Requirements
The following criteria apply to the establishment of the organization offering the service and its basic standing as a legal and operational business entity within its respective jurisdiction or country.

5.5.1 Established Enterprise
The Federation Participant must be a valid legal entity.

5.5.2 Established Service
The Federation Participant must be fully operational in all areas described in the assessment package submitted for assessment.

5.5.3 Legal and Contractual Compliance
The Federation Participant must demonstrate that it understand and complies with all relevant legal requirements, accounting for all jurisdictions and countries within which its services may be used.

5.5.4 Financial Provisions
The Federation Participant must provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried as specified in Section 6 of this document entitled Financial Responsibilities, as well as requirements outlined in the FOPP.
5.6 **OPERATIONAL REQUIREMENTS**

These criteria address the operational requirements for a Federation Participant:

5.6.1 **GENERAL SERVICES DEFINITION**

The Federation Participant must make available to the intended user community a Service Definition that includes all application terms, conditions, and fees, including limitations of its usage.

5.6.2 **DUE NOTIFICATION**

The Federation Participant must have in place and follow appropriate policy and procedures to ensure that it notifies Users in a timely and reliable fashion of any changes to the Service Definition.

5.6.3 **ADHERENCE TO FEDERATION POLICIES**

Through agreement with the Federation Participation Agreement and Addendum, all required policies and practices relevant to the Participant’s Federation Role(s) and Function(s) as described in this document and in the FOPP will be followed.

6 **FINANCIAL RESPONSIBILITIES**

6.1 **INTRODUCTION**

The Financial Responsibilities section defines financial requirements of the Members. Additional information or requirements may be defined by the Foundation.

6.2 **WARRANTY OF PERFORMANCE**

The Foundation warrants the performance of the Management Policies and Administrative processes. CSPs, CMAs, and RPs warrant that:

- MTF Credentials are issued and managed in accordance with MTF Terms of Service;
- Promoted user compliance with MTF requirements;
- Taken all steps required to ensure that a user’s registration attributes have been transferred accurately to a Federation CSP and CMA; and
- They are bound by the terms of relevant party EULAs and/or TOS Agreements.

6.3 **LIABILITY**

RELYING PARTIES ASSUME THE RISK OF POTENTIAL LOSS AND ASSESSING THE PROBABILITY OF LOSS FOR ANY TRANSACTIONS AND INTERACTIONS WITH USERS PRESENTING CREDENTIALS ISSUED UNDER THE MTF. CREDENTIAL SERVICE PROVIDERS ASSUME NO LIABILITY FOR FRAUD OR MISUSE OF THE MTF MINOR’S CREDENTIAL BY MTF USERS OR FALSE POSITIVES OR OTHER ERRORS COMMITTED BY IDENTITY PROVIDERS.

6.4 **INDEMNIFICATION**

MTF DOES NOT INDEMNIFY A RELYING PARTY OR AN INDIVIDUAL USER UNDER THE MTF.
6.5 **INSURANCE**

Credential Service Providers and Identity Providers shall maintain errors and omissions insurance coverage for operations including issuance of credentials and any misidentification that may result from failures to follow the processes described in the MTF.

6.6 **NON REPUDIATION**

MTF credentials are not digital signatures and non-repudiation is not implied by their use.

7 **INTERPRETATION AND ENFORCEMENT**

7.1 **INTRODUCTION**

Interpretation and enforcement defines the legal documents and enforcement mechanisms of the MTF.

7.2 **RELEVANT LEGAL DOCUMENTS**

Availability of Federation identity solutions shall be maintained by meeting appropriate service-level requirements agreed upon by the individuals and organizations that use them. The following legal documents may reference all or portions of the MTF. These include, but are not limited to:

- The Minors Trust Framework (this document)
- Limited Liability Company Agreement of the Generational Trust Alliance
- Bylaws of the Generational Trust Alliance LLC
- Minors Trust Federation: Federation Operating Policies and Practices (this document)
- Generational Trust Alliance Participation Agreement
- Documents Required by all MTF Participants to provide:
  - End User License Agreement and/or Terms of Service
  - Service Level Agreements
  - Insurance Policy
- Documents Required by Relying Parties to provide:
  - Certificate of COPPA Compliance
  - Privacy and Security Policies

7.3 **ENFORCEMENT**

The Foundation will provide ongoing oversight and monitoring of operations, updating of MTF policies, and enforcement of MTF rules, regulations, and agreements.
8 COMPATIBILITY WITH OTHER DIGITAL TRUST NETWORKS

8.1 INTRODUCTION

The MTF is intended to provide a set of principles and rules for the protection of identity and personal data on a digital trust network, as well as provide a mechanism for additional protection of Children afforded under COPPA, for students under FERPA, as well as other legal regimes. The MTF is also intended to maintain compatibility with other digital trust networks whose principles and rules are not in conflict with the MTF. Trust networks wishing to maintain compatibility with the MTF must meet the following rules:

1. It must provide an explicit reference to the current version of the MTF; and
2. It must not define principles or rules that are in conflict with, or requiring an alternate interpretation of, the principles or rules defined in the MTF.

9 GLOSSARY

The following is a list of definitions that may assist a reader in understanding the terms presented in the MTF Identity Management Framework.

Access
The ability to utilize information system resources

Adult
A catch-all term for parents, guardians, teachers or others verified as persons over the age of majority.

Assurance
The fundamental ‘Security Goal.’ Attesting to an entities confidence that the security objectives of integrity, availability, confidentiality and accountability have been adequately met by a specific implementation that performs correctly, offers sufficient protection against unintentional errors (by users or software) and provides sufficient resistance to intentional penetration or by-pass

Assertion
Structured data objects containing Identity information and other relevant data. Sometimes called Identity Assertions

Assessment
An independent review and examination of an entity’s records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures

Attributes
Elements of an Identity

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

Authorization
The official management decision to authorize operation of an information system and to explicitly accept the risk to the company operations (including mission, functions, image, or reputation), company assets, or individuals, based on the implementation of an agreed-upon set of security controls

**Boundary Protection**

The monitoring and control of communications at information systems boundaries to prevent and detect malicious and other unauthorized communication

**Child**

A person under the age of 13. Relying Parties or local law may extend the age for required consent beyond the age of 12 and in the context of this document those individuals requiring consent will also be considered Children.

**Consent Management Authority**

An organization that establishes and manages the consensual relationship between an individual and a Relying Party

**Cookie**

Information supplied by a web server to a browser that is stored temporarily and then returned to the server on any subsequent visits or requests

**Credential**

An object that authoritatively binds an identity (and optionally additional attributes) to a token (i.e. LoginKey) possessed and controlled by a person

**Credential Service Provider**

An independent third party or other trusted entity that registers user tokens, and/or issues an electronic credential to users and may verify the operations of Identify Providers and Attribute Authorities and Consent Management Authorities

**Device ID**

A device ID (device identification) is a distinctive number associated with a smartphone or similar handheld device. Device IDs are separate from hardware serial numbers, but include MAC addresses

**Educator**

An Adult (such as a teacher or a school administrator) who has a job in the field of education, is certified by the State in which they teach, and who seeks parental permission to grant COPPA consents for the purposes of utilizing online services for teaching Children.

**Identity**

A name or digital representation of an individual person that includes sufficient information to ensure that the name is unique

**Identity Attributes**

Information elements relevant to a subject

**Identity Proofing**

The process by which an Identity Provider or Attribute Authority (AA) verifies sufficient information to uniquely identify a person or attributes about a person
Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Jurisdiction

The geographical area to which the authority to pass and enforce laws, rules, and regulations applies. MTF Participants may discover controlling legal jurisdiction through either User self-assertion or via IP address, or both.

Linking

Use of a persistent identifier that can be used to recognize a user over time, or across different Web sites or online services, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service.

Minor

A person under the age of majority, as described by their local jurisdiction and application, such as the ability to contract, view Adult content, or consume restricted products. For the purposes of the MTF, a Minor can be classified as a child (under the age of 13) or a teen (age 13 or over) and thus not protected by COPPA.

Non-repudiation

Providing the sender of information with proof of delivery and providing the recipient with proof of the sender’s identity so that neither can later deny having processed the information.

Ombudsmen

Parental Consent

Parental Consent, for the purposes of the MTF, means consent granted by the parent, guardian, or anyone authorized by the parent or guardian. Parental Consent is reasonably calculated in light of available technology to ensure that the person providing consent is the parent or guardian.

Participant

Organizations which join and maintain their membership in the Minors Trust Foundation.

Password

A secret that a claimant memorizes and uses to authenticate his or her identity.

Personally Identifiable Information (PII):

Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Personal Identification Number (PIN)

A password consisting only of decimal digits.
Privacy
Restricting access or excluding access to information about a subscriber or Service Provider information in accordance with International, Federal and State law and local policy.

Pseudonym
A name that a person or group assumes for a particular purpose, which differs from his or her original or true name.

Registration
The process through which a party applies to become a subscriber of an Identity Provider and a Credential Service Provider validates the identity of that party on behalf of the Identity Provider.

Secure Socket Layer (SSL)
Secure Socket layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that’s transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:”.

Security Assertion Markup Language (SAML)
A specification for encoding security assertions in the Extensible Markup Language (XML).

Security Controls
The management, operational, and technical controls, (i.e., safeguards or countermeasure) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Services Provider
An entity that relies upon the subscriber’s (users) credentials, typically to process a transaction or grant access to information or a system.

Standard
A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.

Token
A physical device (or specialized software on a device such as a mobile phone) used in authentication.

U13
A person under the age of 13. Also, see Child.

Verifiable
To gather enough information to either verify or allow for the future verification such that the information provided is relied upon in the absence of verification.

Verification
The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity system.