

Notes: Continued

11. It is expected that the IDE Authority will authorize performance of the interaction authorization functions, by one or more service providers, following their accreditation by one or more Accreditation Bodies appointed by the Authority.
12. A trusted entity is an entity who has been issued an IDE Trust Credential or Trust Mark. An entity must be in possession of a valid IDE Trust Credential or Trust Mark to perform a trusted interaction or transaction.
13. It is expected that functionality will be required to enable mutual trust to be established between interacting parties.
14. Whether reliance is predominantly one sided or mutual, each relying party will need to specify the lowest IAL they will accept (that the other party must demonstrate); and
15. Their preferred or acceptable MOA's.
16. The Trusted Entity wishing to interact links to the IDE Server for the purpose of entity authentication and disclosure to the relying party of the entities IAL.
17. Authentication should be based upon the data obtained from the entity at the time of enrollment.

Notes: Continued

18. Acceptance by the Relying Party is expected to be based entirely on the result of authentication of the Trusted Entity and IAL of the Trusted Entity disclosed by the IDE Server.
19. To conform to FIPP's, no personal attributes or personal information of the Trusted Entity should be disclosed to the Relying Party prior to a decision being made by both parties to begin trusted interaction.
20. When trusted interaction or transaction begins, each party to the transaction may request disclosure of personal attributes and information in accordance with normal business or social practice.

IDE TRUST COMPONENTS

- Privacy Assurance
- Entity Identity Assurance
- Entity Suitability Assurance
- Entity Authentication Assurance
- IDE Service Provider – Security Assurance
- IDE System – Security Assurance
- IDE Authority – Integrity Assurance
- IDE Transparency Assurance