Notes:

1. Functions performed by the IDE Authority are expected to include: accreditations; contracting for enrollment & authorization services; issuance of IDE Trust Credentials and Trust Marks; detection and management of breaches of trust, security and privacy; management and administration of all IDE Operations.
2. It is expected that the IDE Authority will authorize performance of the enrollment functions, by one or more service providers, following their accreditation by one or more Accreditation Bodies appointed by the Authority.
3. Demands for disclosure of personal attributes and information by human entities must be restricted and justified in accordance with FIPP's.
4. These identity proof and verification functions should be performed in conformance with an IDE Proof and Verification standard.
5. Operations of all service providers authorized to perform enrollment functions should be in conformance with an established, holistic, security assurance standard. That standard should require all service providers to treat all common threats and vulnerabilities as well as those that are unique to each service provider The level of operational threat/attack resistance, to be assured, should be a policy formulated by the IDE Authority.
6. The outcome of enrollment is expected to be issuance of an IDE Trust Credential that certifies that the holding entity has an Identity Assurance Level (IAL) that assurers none or very little, some, high or very high certainty that the claimed identity is valid. For organizations and systems or devices, it may be more appropriate to issue an IDE Trust Mark rather than a credential.

Notes: Continued

7. This function binds the entity to the IDE Identity Credential. It has been termed Authentication Binding because the intent is that the entity will be bound at the time of enrollment and the binding used to Authenticate the entity prior to trusted transaction. The type of binding used should be in accordance with the Method of Authentication (MOA) associated with the entity and IAL. MOA's that may be appropriate could include, simple username/password, Static KBA, Dynamic KBA, biometric measurement or a KBA/biometric combination.
8. An Identity Registration function is expected to be performed following successful verification of identity of an entity to one or more IAL's. It is expected that the registrar will contain the core identity attributes, resolution attributes, binding data (e.g. KBA questions) and an IDE unique identifier.
9. All trusted identity data stored and retrieved during enrollment should be protected in conformance with an IDE data protection standard. That standard should require all service providers to treat all common data threats and vulnerabilities as well as those that are unique to each service provider. The level of resistance to data attacks, to be assured, should be a policy formulated by the IDE Authority.
10. The assumption is made that an IDE server will exist to function as a means to independently authenticate entities wishing to be trusted and to confirm their IAL's.