Trust Level	Expected RP Trust Policies & Criteria	Evidence of Trustworthiness
Can the IDE be Trusted?	• Establishment of a Strong IDE Authority • Lack of Assurance Provider "Hold Harmless" Agreements and Availability of Legal Recourse. • Quality Assurance of Assurance/Service Providers. • Security Assurance of Assurance/Service Providers. • Existence of a Management System for Prevention, Detection & Control of Breaches of Trust, Privacy and Security. • Etc.	• Appointment of Strong IDE Governors/Managers. • Copies of IDE Service/Assurance Provider Model Agreements Showing Lack of Indemnity. • Certificates of Competence Accreditation. • Certificates of Security Assurance Compliance. • Specifications of the Design & Performance Requirements of the System for Management of Trust, Privacy and Security. • Etc.
Can the IDE Systems & Processes be Trusted?	• Use of Sound Entity Identity & Suitability Assurance Standards. • Existence of Threat, Vulnerability & Risk Profiles for all Critical IDE Processes & IT Systems. • Low Entity Assurance and Authentication Failure Rates. • Etc,	• Certificates of Compliance with Assurance Standards Awarded to IDE Assurance providers. • Specification of the measures taken to prevent, treat, resist all credible threats and vulnerabilities. • • Etc.
Can the Entity be Trusted?	• Existence of Comprehensive Methods of Detection and Control of all Known Types and Techniques of Entity Identity & Suitability Fraud and Harmful Acts. • Etc.	• Evidence that Entity Verification and Authentication Standards are based upon rigorous analysis of all known types and techniques of identity and suitability fraud. • Etc.
Can the Entity Trust the RP?	• Existence of a Method that enables an Entity to Know the Assurance Level of a RP in advance of Interaction Authorization. • Etc.	• Specification of the Process for Issuance of IDE Trust-Marks to Relying Parties. • Etc.