ASP Audit Checklist

eSign DIGITAL
Empanelled eSign Service Provider

ASP Audit Checklist

	Audit parameters	
1	The communication between ASP and ESP should be Digitally Signed and encrypted	□
2	Communication line between ASP and ESP should be secured. It is strongly recommended to have leased lines or similar secure private lines between ASP and ESP. If a public network isused, a secure channel such as SSL should be deployed	□
3	ASP should have a documented Information Security policy in line with security s tandards such as ISO 27001.	□
4	Compliance review of controls as per Information security policy	□
5	ASPs should follow standards such as ISO 27000 to maintain Information Security	□
6	Compliance to prevailing laws such as IT Act 2000 should be ensured	□
7	Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional network security controls and end pointauthentication schemes may be put in place.	□
8	Resident consent process must be implemented to obtain consent for every transaction carried out. The user must be asked for willingness to sign it and consent form should be stored .	□
9	Application Security Assessment of the ASP by Cert-in empanelled auditor	□
10	ASP data logging for audit purposes provisioned.	□
11	ASP should not delegate any obligation to external organizations or applications.	□
12	The Domain would belong to the ASP, ownership of domain should belong to ASP	□