#	Assertions	Answer	Comment
	Attribute Management and Attribute Release	☐	
1	The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.	☐	
2	The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.	☐	
3	The AA Operator must collect and publish the community documents for the benefit of Relying Parties.	☐	
	Attribute Assertions	☐	
1	Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.	☐	
2	The AA must respect data protection requirements of the Infrastructure and Community. This may mean that AAs require client authentication, in addition to the encryption of the messages and the communication channel.	☐	
3	If an AA Operator issues assertions containing a lifetime, this lifetime must be compliant with the Community policies, be no more than 24 hours, and the assertion must not be valid beyond the validity period of the attributes it contains. The Community Management is responsible for the content of the assertion, as issued, during its entire lifetime.	☐	
4	Re-issuance of assertions must be based on information held in the AA at the time of re-issuance.	☐	
5	The AA Operator must only issue assertions or release attributes to requesters in accordance with the Community policies.	☐	
	Operational Requirements	☐	
1	An AA that issues attribute assertions must be a dedicated system, running no other services than those needed for the AA operations.	☐	
2	An AA may be run in a virtual environment that has security requirements the same or better than required for the AA, and for all services running in this environment, and it must not leave this security context. Any virtualization techniques employed (including the hosting environment) must not degrade the context as compared to any secured physical setup. Only AA Operator designated personnel should have control over the virtualisation and security context of the AA.	☐	
3	The AA must be located in a secure environment where access is controlled and limited to specific trained personnel.	☐	
4	The AA must be run with an intended continuous availability. Hosted Communities must be informed if AA Operator procedures change.	☐	
5	To achieve sustainability, an AA Operator should offer its AA services as a long term commitment.	☐	
	Key Management	☐	
1	A key used to protect assertions should be dedicated to assertion protection functions.	☐	
2	Keys must not be shared between AA Operators. A single AA Operator may use the same signing key for multiple AAs. Where multiple AAs are under the control of a single AA operator but located in physically distributed locations, the key must only be shared using secure protocols.	☐	
3	Keys must have a protection strength equivalent to 112 bits (symmetric) or higher.	☐	
4	Keys must only be accessible by the service and by trained personnel subject to procedural controls.	☐	
5	AA Operators are encouraged to consider using an HSM to store signing keys. Otherwise, when using software-based private keys these must be suitably protected by the operating system.	☐	

	Network Configuration	☐	
1	The network to which the AA system is connected must be highly protected and suitably monitored.	☐	
	Site security	☐	
1	The AA Operator should document the physical site security controls and maintain them in a state consistent with the security requirements of the hosted Communities.	☐	
	Metadata publication	☐	
1	The AA Operator must publish at least the following metadata for each AA it hosts, to the Community and related relying parties:	☐	
1.a	administrative contact details for the AA Operator, including at least one email address and one postal contact address	☐	
1.b	an operational security contact for the AA Operator, being at least an email address and preferably including a telephone number,	☐	
1.c	those aspects of their operational environment that are relevant to the evaluation of the security and trust by the Communities and Relying Parties	☐	
1.d	the public key for verifying signed messages, where relevant, or the set of certificates up to a self-signed root	☐	
1.e	a web URL to a general information page about the Community	☐	
2	The AA Operator should provide a means to validate the integrity of its roots of trust.	☐	
	Audits	☐	
1	The attributes in the AA and their binding to subjects must be verifiable and auditable.	☐	
2	The AA Operator must record and archive at least the following for all of its hosted AAs	☐	
2.a	all requests for attributes	☐	
2.b	all issued attribute assertions	☐	
2.c	any configuration change to the AA relevant to the access control of the attribute repository	☐	
2.d	any change affecting the binding between subjects and attributes	☐	
3	The AA Operator must record and archive at least the following for of its AA issuance s	☐	
3.a	all login/logout/reboot/key activations of the issuing system	☐	
3.b	changes to the configuration of the issuing system	☐	
4	The AA Operator must keep these records after termination of the effects of the auditable event for as long as required by the Community and any relying parties that have entered into an agreement with the AA Operator, and as required by applicable legislation.	☐	
5	The AA Operator must provide assistance to operational security teams during a security incident.	☐	

6	The AA Operator must accept being audited following reasonable requests from a Community it serves and from relying parties that have entered into an agreement with the AA Operator, to verify its compliance with these guidelines.	☐	
7	The AA Operator should perform operational audits of its staff at least once per year. A list of AA Operator staff should be maintained, and verified at least once per year.	☐	
	Privacy and confidentiality	☐	
1	AA Operators must define and publish an appropriate privacy and data release policy compliant with the relevant legislation and the requirements of the Community.	☐	
	Compromise and disaster recovery	☐	
1	The AA Operator must have an adequate compromise and disaster recovery procedure, and must be willing to disclose this to the hosted Communities or to either an assessor or all related relying parties.	☐	
	Relying Party Obligations	☐	
1	If a Community uses AAs operated by multiple AA Operators then Relying Parties must assess each of the AA Operators individually.	☐	
2	Relying Parties must verify the integrity and validity of attribute assertions and any binding to a valid subject at the time of reliance.	☐	
3	Relying Parties must rely on assertions with an explicit lifetime only for as long as they are valid.	☐	
4	Relying Parties must assess the risk of relying on assertions with no explicit lifetime and should not rely on them for longer than 24 hours after issuance.	☐	
5	Relying Party must validate all verifiable elements.	☐	