# IEEE 2030.5 Protocol (List of Security Properties)

1. If a client PUTs or POSTs a resource to a server containing attributes or elements that instead are to be populated by the server (e.g., href), the server SHALL return an HTTP 400 error.
2. A server MUST respond with a 400 (Bad Request) status code to any HTTP/1.1 request message that lacks a Host header field and to any request message that contains more than one Host header field or a Host header field with an invalid field-value.
3. If a server did not wish a client to know of the existence of the resource, it should instead send a 404 (“Not Found”) response code.
4. The server generating a 401 response MUST send a WWW-authenticate header field containing at least one challenge applicable to the target resource.
5. The origin server MUST generate an Allow header field in a 405 response containing a list of the target resource’s currently supported methods.
6. A client SHALL declare acceptable media types using the HTTP Accept header.
7. Access control lists allow or deny use of resources based on authentication level and address information.
8. Access control list (ACL) attributes represent the data that would be used to hold information to determine whether access to a particular resource by a particular client is allowed or denied.
9. Resource access not requiring application layer authentication, data confidentiality, or integrity checking SHALL occur through requests from a client to the host server using HTTP.
10. The certificate Policy extension in any certificate consists of one or more PolicyInformation objects containing only the policyIdentifier field.
11. In the Manufacturing PKI hierarchy, each device certificate and the CAs that make up the device certificate’s path contain one or more device type identifiers encoded in the certificatePolicy extension in the PolicyInformation: policyIdentifier field.
12. Each certificate, except self-signed client certificates and root certificates, MUST contain an AuthorityKeyIdentifier extension of form [0] KeyIdentifier where the value of the KeyIdentifier field is taken from the value of the SubjectKeyIdentifier extension of the certificate issuer.
13. Per IETF RFC 5280, devices MUST reject any certificate containing unrecognized critical certificate extensions.
14. All devices MUST be able to verify the chain of signatures leading up to any one of the roots.
15. Within the Manufacturing PKI hierarchy, all certificates MUST contain only an EC P-256 public key.

16. Servers SHALL assign a unique Instance label of up to 63 bytes in UTF-8 format for each DNS SRV/TXT record pair that it advertises.
17. Devices SHALL use HTTPS using the port number indicated if the https key is present with a non-empty value.
18. If a secure connection is required for the function set or resource, then the https key SHALL be present in the TXT record.
19. Devices SHALL rediscover URIs upon notification of the server DNS-SD record change or a request fails with a 404 (Not Found) error.
20. Servers SHOULD allow only the end device that corresponds to a given EndDevice resource to modify the Subscriptions within that resource.
21. If a server supports Function Set Assignments, it SHALL support a minimum of one Function Set Assignments for each HAN device registered to the server.
22. Client devices that do not subscribe SHALL query at least once every 24 hours, but SHALL NOT query more than once per hour.
23. When devices are registered to one or more DER Control servers, they SHALL NOT act upon any public DER Control servers that are present in the HAN or become available.
24. DemandResponseProgram server devices SHALL be capable of interacting, storing and supporting at least 1 DemandResponseProgram instance.
25. If a client is not registered to any Pricing server, the client SHALL use the Primacy value of any discovered public Pricing servers for the commodity or commodities of interest.
26. If a resource does not have an ACL, access is granted unconditionally (i.e., open access).
    When an ACL exists, its default configuration means no access is granted unless explicitly allowed by the ACL's settings.
27. The `aclDefaultAccess` entry in each ACL SHALL be applied first to incoming requests regardless of client identity.
28. A SpecificIDDescriptor in the ACL MAY grant additional privileges based on client IP and port; otherwise, defaults apply.
29. ACLs grant privileges but do not explicitly deny them; if a privilege is not granted, it is considered denied.
30. An incoming request is authorized if and only if: Method authorization is true, AuthType authorization is true, DeviceType authorization is true.
31. Method authorization is true if the requested HTTP method bit (e.g., GET, PUT, POST, DELETE, HEAD) is set in the ACL entry's `Method` attribute; else false.
32. AuthType authorization is true if the client's authentication type bit (e.g., 0x8 for device cert) matches at least one bit set in the ACL entry's `AuthType`.
33. DeviceType authorization is true if the ACL entry's `DeviceType` is 0 ("any device type") or matches the device's type from its certificate.
34. If Method authorization fails, the server MAY respond with `400 Bad Request` or `405 Method Not Allowed`.

35. If AuthType or DeviceType authorization fails, the server SHOULD respond with `404 Not Found` or possibly `401 Unauthorized`.
36. Per the default security policy (Clause 6.8), function sets that contain critical data (e.g., DRLC, Metering) SHOULD require device certificate (AuthType=0x8).
37. The EndDeviceList resource is often accessible to any client (Method=GET, AuthType=NoAuth) for a device to locate its own EndDevice entry.
38. If a client fails AuthType or DeviceType checks, the server SHOULD respond with `404 Not Found`, but MAY use `401 Unauthorized`.
39. A device SHALL use DNS-SD (mDNS or xmDNS) to advertise or locate function sets and resources, returning SRV and TXT records with the required keys (`txtvers`, `dcap`, `path`, etc.)