## 2.4 Defined Profile Identifiers

Profile objects (object class CKO\_PROFILE) describe which PKCS #11 profiles the token implements.

The **CKA\_PROFILE** attribute identifies a profile that the token implements.

| **Attribute** | **Data type** | **Meaning** |
| --- | --- | --- |
| CKA\_PROFILE\_ID | CK\_PROFILE\_ID | ID of the supported profile. |

The following table defines the **CK\_PROFILE\_ID** values:

| **Constant** | **Meaning** |
| --- | --- |
| CKP\_INVALID\_ID | Invalid profile |
| CKP\_BASELINE\_PROVIDER | Baseline Provider |
| CKP\_EXTENDED\_PROVIDER | Extended Provider |
| CKP\_AUTHENTICATION\_TOKEN | Authentication Token |
| CKP\_PUBLIC\_CERTIFICATES\_TOKEN | Public Certificates Token |
| CKP\_HKDF\_TLS\_TOKEN | HKDF TLS Token |
| CKP\_VENDOR\_DEFINED | Vendor defined |

## 3.7 HKDF TLS Clause

This profile builds on the PKCS #11 Baseline Provider and/or Baseline Consumer profiles to provide for use of the CKM\_HKDF\_DERIVE\_DATA mechanism in the TLS 1.3 context.

### 3.7.1 Implementation Conformance

An implementation is a conforming HKDF TLS Token if it meets the conditions as outlined in the following section.

### 3.7.2 Conformance of an Authentication Token

An implementation conforms to this specification as an HKDF TLS Token if it meets the following conditions:

1. If the implementation is a consumer then it SHALL support the conditions required by the PKCS #11 Baseline Consumer Clause (Section 3.2)
2. If the implementation is a provider then it SHALL support the conditions required by the PKCS #11 Baseline Provider Clause (Section 3.3)
3. Supports the following data types:
   1. CK\_HKDF\_PARAMS (PKCS11-Curr 2.62.2)
4. Supports the following attributes:
   1. None specified
5. Supports the following objects:
   1. CKO\_DATA ([PKCS11-Base] 4.5)
   2. CKO\_SECRET\_KEY ([PKCS11-Base] 4.10)
   3. CKO\_PROFILE ([PKCS11-Base] 4.13) with value CKP\_HKDF\_TLS\_TOKEN
6. Supports the following functions:
   1. C\_Derive ([PKCS11-Base] 5.6)
7. Supports the following mechanisms:
   1. CKM\_HKDF\_DATA (PKCS11-Curr 2.62.4)
      1. The Provider must not reject derive request based on the pInfo value if the following pInfo values are given:
         1. The string L1,L2,”tls iv”,0 (L1, L2, 0x74, 0x6c, 0x73, 0x20, 0x69, 0x76, 0x00) where L1 is the most significant byte of CKA\_KEY\_LENGTH and L2 is the least significant byte of CKA\_KEY\_LENGTH.
         2. The string L1,L2,”tls quic iv”,0 (L1, L2, 0x74, 0x6c, 0x73, 0x20, 0x71, 0x75, 0x69, 0x63, 0x20, 0x69, 0x76, 0x00) where L1 is the most significant byte of CKA\_KEY\_LENGTH and L2 is the least significant byte of CKA\_KEY\_LENGTH.
      2. The Provider can accept other values for pInfo.
8. Optionally supports any clause within [PKCS11-Base] that is not listed above
9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined extensions, conformance clauses) that do not contradict any PKCS #11 requirements.