

FEATURE / PRODUCT	Basic Personal ID	Basic Enterprise ID	Basic Team ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	BASIC_PERSONAL_ID_1	BASIC_ENTERPRISE_ID_1	BASIC_TEAM_ID_1
2-year	BASIC_PERSONAL_ID_2	BASIC_ENTERPRISE_ID_2	BASIC_TEAM_ID_2
3-year	BASIC_PERSONAL_ID_3	BASIC_ENTERPRISE_ID_3	BASIC_TEAM_ID_3
4-year	BASIC_PERSONAL_ID_4	BASIC_ENTERPRISE_ID_4	BASIC_TEAM_ID_4
5-year	BASIC_PERSONAL_ID_5	BASIC_ENTERPRISE_ID_5	BASIC_TEAM_ID_5
SET BY TSP	UI SUPPORT / P12 (-PIN) DELIVERY OPTION		
PKCS#10 via GUI + CMP	yes	yes	yes
p12 via GUI / PIN: mobile SMS	yes	yes	yes
p12 via GUI / PIN: hard copy mail	no	no	no
SET BY TSP	KEY USAGE		
digitalSignature	yes	yes	yes
keyEncipherment	yes	yes	yes
dataEncipherment	yes	yes	yes
nonRepudiation	no	no	no
SET BY TSP	EXTENDED KEY USAGE		
clientAuth	yes	yes	yes
serverAuth	no	no	no
emailProtection	yes	yes	yes
SET BY CUSTOMER	MANDATORY SUBJECT FIELDS I		
SAN rfc822Name=eMail	yes	yes	yes
SAN dnsName	no	no	no
Wildcard Option	no	no	no
SAN otherName / principalN	optional 0...1	optional 0...1	optional 0...1
SAN registeredID	optional 0...1	optional 0...1	optional 0...1
SAN iPAddress 4	no	no	no
SAN iPAddress 6	no	no	no
organizationName (O)	no	yes	yes
organizationalUnit (OU)	no	optional 0...3	optional 0...3
givenName (GN)	yes	yes	no
surName (SN)	yes	yes	no
Street Address	no	no	no
Postal Code	no	no	no
Locality (L)	no	yes	yes
State (S)	no	yes	yes
Country (C)	yes	yes	yes
commonName (CN)	yes (=SN+GN)	yes (=SN+GN)	yes (=O)
SET BY TSP	MANDATORY SUBJECT FIELDS II		
subjectSerialNo.	yes	yes	yes
2.5.4.97 organizationIdentifier	no	no	no
2.5.4.15 businessCategory	no	no	no
1.3.6.1.4.1.311.60.2.1.1 jurisdictionLocalityN	no	no	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionStateOrProvinceN	no	no	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionCountryN	no	no	no
SET BY TSP	PKI INFORMATION		
Root distribution process	customer deployment	customer deployment	customer deployment
Root CA	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuing CA	D-TRUST Limited Basic CA 1-3 2019	D-TRUST Limited Basic CA 1-3 2019	D-TRUST Limited Basic CA 1-3 2019
Issuing CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Issuing CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
EE key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Policy Level	n/a	n/a	n/a
SET BY TSP	REFUND POLICY		
7 days	yes	yes	no
30 days	no	no	yes

FEATURE / PRODUCT	Basic Enterprise SIG ID	Basic Enterprise AUT ID	Basic Enterprise ENC ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	BASIC_ENTERPRISE_SIG_ID_1	BASIC_ENTERPRISE_AUT_ID_1	BASIC_ENTERPRISE_ENC_ID_1
2-year	BASIC_ENTERPRISE_SIG_ID_2	BASIC_ENTERPRISE_AUT_ID_2	BASIC_ENTERPRISE_ENC_ID_2
3-year	BASIC_ENTERPRISE_SIG_ID_3	BASIC_ENTERPRISE_AUT_ID_3	BASIC_ENTERPRISE_ENC_ID_3
4-year	BASIC_ENTERPRISE_SIG_ID_4	BASIC_ENTERPRISE_AUT_ID_4	BASIC_ENTERPRISE_ENC_ID_4
5-year	BASIC_ENTERPRISE_SIG_ID_5	BASIC_ENTERPRISE_AUT_ID_5	BASIC_ENTERPRISE_ENC_ID_5
SET BY TSP	UI SUPPORT / P12 (-PIN) DELIVERY OPTION		
PKCS#10 via GUI + CMP	yes	yes	yes
p12 via GUI / PIN: mobile SMS	yes	yes	yes
p12 via GUI / PIN: hard copy mail	no	no	no
SET BY TSP	KEY USAGE		
digitalSignature	yes	yes	no
keyEncipherment	no	no	yes
dataEncipherment	no	no	yes
nonRepudiation	no	no	no
SET BY TSP	EXTENDED KEY USAGE		
clientAuth	yes	yes	no
serverAuth	no	no	no
emailProtection	yes	no	yes
SET BY CUSTOMER	MANDATORY SUBJECT FIELDS I		
SAN rfc822Name=eMail	yes	yes	yes
SAN dnsName	no	no	no
Wildcard Option	no	no	no
SAN otherName / principalN	optional 0..1	optional 0..1	optional 0..1
SAN registeredID	optional 0..1	optional 0..1	optional 0..1
SAN iPAddress 4	no	no	no
SAN iPAddress 6	no	no	no
organizationName (O)	yes	yes	yes
organizationalUnit (OU)	optional 0..3	optional 0..3	optional 0..3
givenName (GN)	yes	yes	yes
surName (SN)	yes	yes	yes
Street Address	no	no	no
Postal Code	no	no	no
Locality (L)	yes	yes	yes
State (S)	yes	yes	yes
Country (C)	yes	yes	yes
commonName (CN)	yes (=SN+GN)	yes (=SN+GN)	yes (=SN+GN)
SET BY TSP	MANDATORY SUBJECT FIELDS II		
subjectSerialNo.	yes	yes	yes
2.5.4.97 organizationIdentifier	no	yes	yes
2.5.4.15 businessCategory	no	no	no
1.3.6.1.4.1.311.60.2.1.1 jurisdictionLocalityN	no	no	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionStateOrProvinceN	no	no	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionCountryN	no	no	no
SET BY TSP	PKI INFORMATION		
7 days	customer deployment	customer deployment	customer deployment
30 days	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuing CA	D-TRUST Limited Basic CA 1-3 2019	D-TRUST Limited Basic CA 1-3 2019	D-TRUST Limited Basic CA 1-3 2019
Issuing CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Issuing CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
EE key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Policy Level	n/a	n/a	n/a
SET BY TSP	REFUND POLICY		
7 days	yes	yes	yes
30 days	no	no	no

STRUCTURE / PRODUCT	Basic Device ID	Basic Seal ID	
BY TSP			API PRODUCT CODE
days validity period	no	no	
ear	BASIC_DEVICE_ID_1	BASIC_SEAL_ID_1	
ear	BASIC_DEVICE_ID_2	BASIC_SEAL_ID_2	
ear	BASIC_DEVICE_ID_3	BASIC_SEAL_ID_3	
ear	BASIC_DEVICE_ID_4	BASIC_SEAL_ID_4	
ear	BASIC_DEVICE_ID_5	BASIC_SEAL_ID_5	
BY TSP			UI SUPPORT / P12 (-PIN) DELIVERY OPTION
S#10 via GUI + CMP	yes	yes	
via GUI / PIN: mobile SMS	yes	yes	
via GUI / PIN: hard copy mail	no	no	
BY TSP			KEY USAGE
taSignature	yes	yes	
Encipherment	yes	no	
aEncipherment	yes	no	
Repudiation	no	yes	
BY TSP			EXTENDED KEY USAGE
ntAuth	yes	no	
verAuth	no	no	
ailProtection	no	no	
BY CUSTOMER			MANDATORY SUBJECT FIELDS I
rfc822Name=eMail	no	no	
dnsName	optional 0...1	no	
Wildcard Option	no	no	
otherName / principalN	no	no	
registeredID	optional 0...1	no	
IPAddress 4	optional 0...1	no	
IPAddress 6	optional 0...1	no	
organizationName (O)	yes	yes	
organizationalUnit (OU)	optional 0...3	optional 0...1	
enName (GN)	no	no	
Name (SN)	no	no	
et Address	no	no	
tal Code	no	no	
ality (L)	yes	yes	
te (S)	yes	yes	
ntry (C)	yes	yes	
hmonName (CN)	yes (=Any or =O)	yes=O	
BY TSP			MANDATORY SUBJECT FIELDS II
jectSerialNo.	yes	yes	
4.97 organizationIdentifier	no	yes	
4.15 businessCategory	no	no	
6.1.4.1.311.60.2.1.1 sdictionLocalityN	no	no	
6.1.4.1.311.60.2.1.2 sdictionStateOrProvinceN	no	no	
6.1.4.1.311.60.2.1.2 sdictionCountryN	no	no	
BY TSP			PKI INFORMATION
ays	customer deployment	customer deployment	
days	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019	
t CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
t CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
ing CA	D-TRUST Limited Basic CA 1-2 2019	D-TRUST Limited Basic CA 1-3 2019	
ing CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
ing CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
key length	2048 Bit (RSA)	2048 Bit (RSA)	
cy Level	n/a	n/a	
BY TSP			REFUND POLICY
ays	no	no	
days	yes	yes	

FEATURE / PRODUCT	Basic Domain SSL ID*	Basic SSL ID	
SET BY TSP			API PRODUCT CODE
30-days validity period	no	no	
1-year	BASIC_DOMAIN_SSL_ID_1	BASIC_SSL_ID_1	
2-year	BASIC_DOMAIN_SSL_ID_2	BASIC_SSL_ID_2	
3-year	BASIC_DOMAIN_SSL_ID_3	BASIC_SSL_ID_3	
4-year	BASIC_DOMAIN_SSL_ID_4	BASIC_SSL_ID_4	
5-year	BASIC_DOMAIN_SSL_ID_5	BASIC_SSL_ID_5	
SET BY TSP			UI SUPPORT / P12 (-PIN) DELIVERY OPTION
PKCS#10 via GUI + CMP	yes	yes	
p12 via GUI / PIN: mobile SMS	no	no	
p12 via GUI / PIN: hard copy mail	no	no	
SET BY TSP			KEY USAGE
digitalSignature	yes	yes	
keyEncipherment	yes	yes	
dataEncipherment	no	no	
nonRepudiation	no	no	
SET BY TSP			EXTENDED KEY USAGE
clientAuth	yes	yes	
serverAuth	yes	yes	
emailProtection	no	no	
SET BY CUSTOMER			MANDATORY SUBJECT FIELDS I
SAN rfc822Name=eMail	no	no	
SAN dnsName	yes (1...50)	yes (1...50)	
Wildcard Option	yes	yes	
SAN otherName / principalN	no	no	
SAN registeredID	no	no	
SAN iPAddress 4	no	no	
SAN iPAddress 6	no	no	
organizationName (O)	no	yes	
organizationalUnit (OU)	no	optional 0...3	
givenName (GN)	no	no	
surName (SN)	no	no	
Street Address	no	no	
Postal Code	no	no	
Locality (L)	no	yes	
State (S)	no	yes	
Country (C)	no	yes	
commonName (CN)	optional (=SAN1 dnsN)	yes (=SAN1 dnsN)	
SET BY TSP			MANDATORY SUBJECT FIELDS II
subjectSerialNo.	yes	yes	
2.5.4.97 organizationIdentifier	no	no	
2.5.4.15 businessCategory	no	no	
1.3.6.1.4.1.311.60.2.1.1 jurisdictionLocalityN	no	no	
1.3.6.1.4.1.311.60.2.1.2 jurisdictionStateOrProvinceN	no	no	
1.3.6.1.4.1.311.60.2.1.2 jurisdictionCountryN	no	no	
SET BY TSP			PKI INFORMATION
7 days	customer deployment	customer deployment	
30 days	D-TRUST Limited Basic Root CA 1 2019	D-TRUST Limited Basic Root CA 1 2019	
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
Issuing CA	D-TRUST Limited Basic CA 1-2 2019	D-TRUST Limited Basic CA 1-2 2019	
Issuing CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
Issuing CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
EE key length	secp384r1 / 2048 Bit (RSA)+	2048 Bit (RSA)	
Policy Level	n/a	n/a	
SET BY TSP			REFUND POLICY
7 days	no	no	