performio.

D-TRUST | Ein Unternehmen der Bundesdruckerei

FEATURE / PRODUCT	Advanced Personal ID	Advanced Enterprise ID	Advanced Team ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	ADVANCED_PERSONAL_ID_1	ADVANCED_ENTERPRISE_ID_1	ADVANCED_TEAM_ID_1
2-year	ADVANCED_PERSONAL_ID_2	ADVANCED_ENTERPRISE_ID_2	ADVANCED_TEAM_ID_2
3-year	no	no	no
4-year	no	no	no
5-year	no	no	no
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	software vendor	software vendor	software vendor
Root CA	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuing CA	D-TRUST Application Certificates CA 3-1 2013	D-TRUST Application Certificates CA 3-1 2013	D-TRUST Application Certificates CA 3-1 2013
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	ETSI EN 319 411-1 / LCP	ETSI EN 319 411-1 / LCP	ETSI EN 319 411-1 / LCP
SET BY TSP	REFUND POLICY		
7 days	yes	yes	yes
30 days	no	no	no

performio.

D-TRUST | Ein Unternehmen der Bundesdruckerei

FEATURE / PRODUCT	Advanced Enterprise SIG ID	Advanced Enterprise AUT ID	Advanced Enterprise ENC ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	ADVANCED_ENTERPRISE_SIG_ID_1	ADVANCED_ENTERPRISE_AUT_ID_1	ADVANCED_ENTERPRISE_ENC_ID_1
2-year	ADVANCED_ENTERPRISE_SIG_ID_2	ADVANCED_ENTERPRISE_AUT_ID_2	ADVANCED_ENTERPRISE_ENC_ID_2
3-year	no	no	no
4-year	no	no	no
5-year	no	no	no
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	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	software vendor	software vendor	software vendor
Root CA	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuing CA	D-TRUST Application Certificates CA 3-1 2013	D-TRUST Application Certificates CA 3-1 2013	D-TRUST Application Certificates CA 3-1 2013
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	ETSI EN 319 411-1 / LCP	ETSI EN 319 411-1 / LCP	ETSI EN 319 411-1 / LCP
SET BY TSP	REFUND POLICY		
7 days	yes	yes	yes
30 days	no	no	no

performio.

D-TRUST | Ein Unternehmen der Bundesdruckerei

FEATURE / PRODUCT	Advanced Device ID	Advanced Seal ID	
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	
1-year	ADVANCED_DEVICE_ID_1	ADVANCED_SEAL_ID_1	
2-year	ADVANCED_DEVICE_ID_2	ADVANCED_SEAL_ID_2	
3-year	no	no	
4-year	no	no	
5-year	no	no	
SET BY TSP	UI SUPPORT / P12 (-PIN) DELIVERY OPTION		
PKCS#10 via GUI + CMP	yes	yes	
p12 via GUI / PIN: mobile SMS	yes	yes	
p12 via GUI / PIN: hard copy mail	no	yes	
SET BY TSP	KEY USAGE		
digitalSignature	yes	yes	
keyEncipherment	yes	no	
dataEncipherment	yes	no	
nonRepudiation	no	yes	
SET BY TSP	EXTENDED KEY USAGE		
clientAuth	yes	no	
serverAuth	no	no	
emailProtection	no	no	
SET BY CUSTOMER	MANDATORY SUBJECT FIELDS I		
SAN rfc822Name=eMail	no	no	
SAN dnsName	optional 0...1	no	
Wildcard Option	no	no	
SAN otherName / principalN	no	no	
SAN registeredID	optional 0...1	no	
SAN iPAddress 4	optional 0...1	no	
SAN iPAddress 6	optional 0...1	no	
organizationName (O)	yes	yes	
organizationalUnit (OU)	optional 0...3	optional 0...1	
givenName (GN)	no	no	
surName (SN)	no	no	
Street Address	no	no	
Postal Code	no	no	
Locality (L)	yes	yes	
State (S)	yes	yes	
Country (C)	yes	yes	
commonName (CN)	yes (=Any or =O)	yes=O	
SET BY TSP	MANDATORY SUBJECT FIELDS II		
subjectSerialNo.	yes	yes	
2.5.4.97 organizationIdentifier	no	yes	
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		
Root distribution process	software vendor	software vendor	
Root CA	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013	
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
Issuing CA	D-TRUST Application Certificates CA 3-1 2013	D-TRUST Application Certificates CA 3-1 2013	
Issuing CA key length	2048 Bit (RSA)	2048 Bit (RSA)	
Issuing CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	
EE key length	2048 Bit (RSA)+	2048 Bit (RSA)+	
Policy Level	ETSI EN 319 411-1 / LCP	ETSI EN 319 411-1 / LCP	
SET BY TSP	REFUND POLICY		
7 days	no	no	
30 days	yes	yes	

performio.

D-TRUST | Ein Unternehmen der Bundesdruckerei

FEATURE / PRODUCT	Advanced DV SSL ID*	Advanced SSL ID	Advanced EV SSL ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	ADVANCED_DV_SSL_ID_1	ADVANCED_SSL_ID_1	ADVANCED_EV_SSL_ID_1
2-year	ADVANCED_DV_SSL_ID_2	ADVANCED_SSL_ID_2	ADVANCED_EV_SSL_ID_2
3-year	no	no	no
4-year	no	no	no
5-year	no	no	no
SET BY TSP	UI SUPPORT / P12 (-PIN) DELIVERY OPTION		
PKCS#10 via GUI + CMP	yes	yes	yes
p12 via GUI / PIN: mobile SMS	no	no	no
p12 via GUI / PIN: hard copy mail	no	no	no
SET BY TSP	KEY USAGE		
digitalSignature	yes	yes	yes
keyEncipherment	yes	yes	yes
dataEncipherment	no	no	no
nonRepudiation	no	no	no
SET BY TSP	EXTENDED KEY USAGE		
clientAuth	yes	yes	yes
serverAuth	yes	yes	yes
emailProtection	no	no	no
SET BY CUSTOMER	MANDATORY SUBJECT FIELDS I		
SAN rfc822Name=eMail	no	no	no
SAN dnsName	yes (1...50)	yes (1...50)	yes (1...50)
Wildcard Option	yes	yes	no
SAN otherName / principalN	no	no	no
SAN registeredID	no	no	no
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)	no	no	no
surName (SN)	no	no	no
Street Address	no	no	yes
Postal Code	no	no	yes
Locality (L)	no	yes	yes
State (S)	no	yes	yes
Country (C)	no	yes	yes
commonName (CN)	optional (=SAN1 dnsN)	yes (=SAN1 dnsN)	yes (=SAN1 dnsN)
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	yes
1.3.6.1.4.1.311.60.2.1.1 jurisdictionLocalityN	no	no	yes (if applicable)
1.3.6.1.4.1.311.60.2.1.2 jurisdictionStateOrProvinceN nicht verfügbar	no	no	yes (if applicable)
1.3.6.1.4.1.311.60.2.1.2 jurisdictionCountryN	no	no	yes
SET BY TSP	PKI INFORMATION		
Root distribution process	software vendor	software vendor	software vendor
Root CA	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013	D-TRUST Root Class 3 CA 2 EV 2009
Root CA key length	2048 Bit (RSA)	2048 Bit (RSA)	2048 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuing CA	D-TRUST SSL CA 2 2020	D-TRUST SSL Class 3 CA 1 2009	D-TRUST SSL Class 3 CA 1 EV 2009
Issuing CA key length	secp384r1	2048 Bit (RSA)	2048 Bit (RSA)
Issuing CA signaturealgorithm	ecdsa-with-SHA384	sha256WithRSAEncryption	sha256WithRSAEncryption
EE key length	secp384r1 / 2048 Bit (RSA)+	2048 Bit (RSA)+	2048 Bit (RSA)+
Policy Level	EN 319 411-1 / DVCP	EN 319 411-1 / OVCP	319 411-1 / EVCP
SET BY TSP	REFUND POLICY		
7 days	no	no	no
30 days	yes	yes	yes

performio.

D-TRUST | Ein Unternehmen der Bundesdruckerei

FEATURE / PRODUCT	Qualified EV SSL ID	Qualified Website PSD2 ID	Qualified Seal PSD2 ID
SET BY TSP	API PRODUCT CODE		
30-days validity period	no	no	no
1-year	QUALIFIED_EV_SSL_ID_1	QUALIFIED_WEBSITE_PSD2_ID_1	QUALIFIED_SEAL_PSD2_ID_1
2-year	QUALIFIED_EV_SSL_ID_2	QUALIFIED_WEBSITE_PSD2_ID_2	QUALIFIED_SEAL_PSD2_ID_2
3-year	no	no	no
4-year	no	no	no
5-year	no	no	no
SET BY TSP	UI SUPPORT / P12 (-PIN) DELIVERY OPTION		
PKCS#10 via GUI + CMP	yes	yes	yes
p12 via GUI / PIN: mobile SMS	no	no	no
p12 via GUI / PIN: hard copy mail	no	no	no
SET BY TSP	KEY USAGE		
digitalSignature	yes	yes	yes
keyEncipherment	yes	yes	no
dataEncipherment	no	no	no
nonRepudiation	no	no	yes
SET BY TSP	EXTENDED KEY USAGE		
clientAuth	yes	yes	no
serverAuth	yes	yes	no
emailProtection	no	no	no
SET BY CUSTOMER	SUBJECT FIELDS I		
SAN rfc822Name=eMail	no	no	no
SAN dnsName	yes (1…50)	yes (1…50)	no
Wildcard Option	no	no	no
SAN otherName / principalN	no	no	no
SAN registeredID	no	no	no
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…1
givenName (GN)	no	no	no
surName (SN)	no	no	no
Street Address	yes	yes	optional
Postal Code	yes	yes	optional
Locality (L)	yes	yes	yes
State (S)	yes	yes	optional
Country (C)	yes	yes	yes
commonName (CN)	optional (=SAN1 dnsN)	yes (=SAN1 dnsN)	yes=O
SET BY TSP	SUBJECT FIELDS II		
subjectSerialNo.	yes	yes	yes
2.5.4.97 organizationIdentifier	no	no	yes
2.5.4.15 businessCategory	yes	no	no
1.3.6.1.4.1.311.60.2.1.1 jurisdictionLocalityN	yes (if applicable)	yes (if applicable)	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionStateOrProvinceN	yes (if applicable)	yes (if applicable)	no
1.3.6.1.4.1.311.60.2.1.2 jurisdictionCountryN	yes	no	no
SET BY TSP	PKI INFORMATION		
Root distribution process	software vendor / EU TSL	EU TSL	EU TSL
Root CA	D-TRUST Root Class 3 CA 2 EV 2009	D-TRUST Root CA 2 2018	D-TRUST Root CA 2 2018
Root CA key length	2048 Bit (RSA)	4096 Bit (RSA)	4096 Bit (RSA)
Root CA signaturealgorithm	sha256WithRSAEncryption	sha512WithRSAEncryption	sha512WithRSAEncryption
Issuing CA	D-TRUST CA 2-2 EV 2016	D-TRUST CA 2-1 2018	D-TRUST CA 2-2 2019
Issuing CA key length	2048 Bit (RSA)	4096 Bit (RSA)	4096 Bit (RSA)
Issuing CA signaturealgorithm	sha256WithRSAEncryption	sha512WithRSAEncryption	sha512WithRSAEncryption
EE key length	2048 Bit (RSA)+	2048 Bit (RSA)+	3072 Bit (RSASSA-PSS)+
Policy Level	319 411-2 / QCP-w	319 411-2 / QCP-w (+PSD2)	319 411-2 / QCP-L (+PSD2)
SET BY TSP	REFUND POLICY		
7 days	no	no	no
30 days	yes	yes	yes