Statement types and descriptions
0. Introduction
This document contains the standard terms and conditions for the Commfides certificates and EU qualified certificates for electronic signatures, encryption and authentication issued to legal person, (hereinafter referred to as the certificate). The terms and conditions apply to the supplier (hereinafter referred to as Commfides or as the TSP*) and the customer (hereinafter referred to as the subscriber). The customer is responsible for the use of its certificate. The certificates and the terms and conditions are considered accepted when the customer has ordered the certificate. *TSP is the Trusted Service Provider who is the issuer of the certificate and is the overall responsible entity for the certification services. This English version of the PDS supersedes versions in other languages.
1. TSP contact info:
TSP: Commfides Norge AS (business number 988 312 495) Post address: Post box 405, 1327 Lysaker, Norway Visit address: Fornebuveien 1, 1366 Lysaker Website: www.commfides.com Telephone: +47 21 55 62 60 e-mail: servicedesk@commfides.com To request a revocation of the certificate either; Use the TSP webservice if applicable for you; Send an e-mail to sperring@commfides.com and identify yourself and your purpose; Call at +47 21 55 62 80 or; meet up at Commfides premises during office hour. The revocation service on e-mail and phone is available 24/7.
2. Certificate type, validation procedures and usage:
Certificate type: Applies for certificates and qualified certificates signed by subordinate CA certificate “CPN Enterprise-Norwegian SHA256 CA CLASS 3” issued to legal persons. These digital certificates conform to RFC 5280 and utilize the ITU-T X.509 version 3 digital certificate standards. **Validation procedures:** According to the CP/CPS for the certificate, the subject and or subscriber identified in the certificate shall be the one controlling the certificate and be the one with simultaneous access to both the certificate and its activation code (PIN). In order to accomplish this requirement the TSP has restrict validation methods to ensure that only the rightful subject (identified in the certificate) is the one receiving both activation code and certificate. The TSP ensures by the physical presence of the subject or subscriber (or shall have been checked indirectly using means which provides equivalent assurance to physical presence) that the rightful person is the one receiving the certificate (and/or) the activation code. The TSP records and verifies the subject’s and/or the subscriber’s signature and identity document and check the correctness of its personal information. The information is verified in relation to “Det sentrale folkeregister” DSF (National Registry of Persons) or equivalent international registry. The legal person being the subject identified in the certificate is to be identified in the certificate application by full name and organization number of the subject. The subject shall be registered and have a valid status in the national Brønnøysundregistrene or other applicable identification practices. The name and organization number from the certificate application must be consistent with the national Brønnøysundregistrene or other applicable identification practices. The CP/CPS gives more details regarding the validation procedures included the methods for validation of the subscriber if not the same as the subject and the validation of different roles and their relations). Accepted identity documents are: Passport and national identity cards. The TSP may on its own discretion refuse the acceptance of any identity document. (Normally based on security considerations).
3. Reliance limits:
Limitation of use: The certificate is only to be used for PKI based services. The key usage for the end-user certificates is set in the certificate profiles in the "Key Usage" field" and in the "Extended Key

Usage" see "Appendix 3, Commfides Certificate Profiles" in the CP/CPS

The TSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations in its CP/CPS (CP/CPS as indicated section “Applicable agreements, CPS, CP:” below). This liability for damage is limited to maximum 10000, - NOK and applies only to direct loss for the customer not for indirect loss caused by the incident.

The intention or negligence of the TSP is presumed unless that the TSP proves that the damage occurred without the intention or negligence of the TSP. TSP is not liable for damages arising from the use of services exceeding the indicated limitations above and exceeding of the obligation of subscriber and subject indicated in “4. Obligation of subscriber and subject” below.

4. Obligations of subscribers and subject:

A subscriber is a legal or natural person bound by agreement with a trust service provider to any subscriber obligations. The subscriber shall fulfil all obligations of the subscriber agreement. The subject shall fulfil all obligations of the subject agreement. If the subscriber and subject are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject.

The subscriber shall:

a) Submit accurate and complete information to the TSP in accordance with the requirements in the certification practice statement.
b) Maintain the correct information about the subscriber and subject, and notify the TSP of any changes to this information.
c) Notify the TSP if any information in the Certificate is incorrect.
d) Request the certificate to be revoked when a valid revocation reason exists.
e) In the case of being informed that the CA has been compromised, ensure that the private key is no longer used by the subject.
f) Inform the TSP if an authorized subscriber representative no longer is authorized to represent the subscriber.
g) Exercise reasonable care to avoid unauthorized use of the subjects’ private keys.
Particularly keep the activation data (PIN) secret
h) Ensure that restrictions on the subject’s private key and the certificate are kept at all times.
i) Ensure that the use of the subject private keys is immediately and permanently discontinued in case of private key compromise. For instance if control of the subject private keys are lost.
j) Cease the use of the private keys at the end of the key usage periods (use for key decipherment is accepted).
k) Ensure the key pair is only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person. Limitation is notified in each certificate associated PDS;
l) Use and maintain the subject's private key under the subject's sole control.
m) Use the subject's private key(s) for cryptographic functions within the secure cryptographic device. Digital seal shall only be created by the QSCD device. (only applicable for the certificate with the certificate policy QCP-l-qscd)
n) Ensure that use of the certificate is under subscriber control by recording all entities that use and have access to the private keys, included processes, systems and individuals.
o) Notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: i) the subject's private key has been lost, stolen, potentially compromised or; ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.

The subject shall act according to the following points ; a), d), e) g), h), i) , j), k) l) m) o)
(If the subscriber is the same entity as the subject, then all the subscriber obligations apply to the subject as well).

5. Certificate status checking obligations of relying parties:

Relying parties are entitled to, when the certificate is used in a service, to check a certificate’s status using the CRL and/ or the OCSP service related to that specific certificate to verify if a certificate is revoked and to see the status of the certificate being used. (The obligation to relying parties is described in more details in the CP/CPS).

6. Limited warranty and disclaimer/Limitation of liability:

See «3. Reliance limits:»

7. Applicable agreements, CPS, CP:

The applicable CP/CPS for this certificate is to be found here: https://pds.commfides.com/v1-2/Commfides-CP-and-CPS-for-Certificates-and-EU-Qualified-Certificates-Legal-Person-Central_v1-2.pdf named “Commfides-CP-and-CPS-for-Certificates-and-EU-Qualified-Certificates-Legal-Person-Central”. Certificate Policy Identifier: (ETSI EN 319 411-1 [NCP+ NCP and LCP] and ETSI EN 319 411-2 [QCP-l-qscd and QCP-l] (all for legal person)).
NCP+:2.16.578.1.29.13.10.X.X, QCP-l-qscd: 2.16.578.1.29.13.11.X.X, NCP+: 2.16.578.1.29.13.12.X.X, NCP:2.16.578.1.29.13.20.X.X, QCP-l: 2.16.578.1.29.13.21.X.X, NCP: 2.16.578.1.29.13.22.X.X, LCP:2.16.578.1.29.13.30.X.X, LCP: 2.16.578.1.29.13.31.X.X, LCP: 2.16.578.1.29.13.32.X.X. The “X” implies digits for the latest versions.

8. Privacy policy:

The TSP is undertaking technical and organizational measures against unauthorized and unlawful processing of personal data and

against accidental loss and destruction of, and damage to, personal data.

Records associated with a certificate (including information used under registration, subject device provision both from subscriber and subject, any subsequent revocation, the identity and any specific attributes placed in the certificate) are retained for at least Ten (10) years following the date the Certificate expires or is revoked. These records may be passes to third parties under the same conditions as required by the existing CP and CPS in the case of the TSP terminating its services.

The following information/records are kept confidential and private (treated as private): CA application records, whether approved or disapproved; Certificate application records; Transactional records and the audit trail of transactions;

The following information/records are not considered confidential or private:
Certificates and their belonging public keys. Certificates and their belonging public key is public available at the TSP's LDAP service.
Certificate status. A certificate's status is public available at the TSP's CRL and OCSP service.

9. Refund policy:

Purchase of the TSP certificates may either be consumer purchases or commercial purchases. Consumer purchases are certificates sold to a private person, commercial purchases is sale to a legal business.
For consumer purchase the agreement are subject to the rules for consumer purchases «Lov om forbrukerkjøp (forbrukerkjøpsloven)" If the customer cancels the purchase after the certificate is sent from the TSP's distribution, the customer are charged a fee for the distribution of the certificate according to the current price list on https://www.commfides.com

For all other purchases the refund policy, if any, is stated in agreement between the TSP and the customer.

10. Applicable law, complaints and dispute resolution:

Procedure for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters:

In order to have a complaint/dispute processed by the TSP the customer/subscriber are obligated to;

- In cases regarding certificates issued to legal persons whereas the certificate has been sold through one of the TSP's distributors, the complaint/ dispute shall be submitted by this distributor.
- The complaint/ dispute shall clearly identify involved services/certificate(s), time of incident, grounds for complaints/dispute. The complaint/ dispute shall be sent to servicedesk@commfides.com

The TSP is obligated to; Confirm the receipt of the complaints/dispute; Process the complaint/dispute and within reasonable time respond with the outcome of the process or invite to further negotiation.

Disputes between the TSP and its customers are aimed to be solved in amiability negotiations between the parties. Disputes, if required, are to be solved in the court of "Asker og Bærum Tingrett". The relationship between the customer and the TSP is regulated by Norwegian laws.

Governing Law:
Subject to any limits appearing in applicable law, the laws of the Kingdom of Norway.

11. TSP and repository licenses, trust marks, and audit:

Commfides Norge AS (Commfides) is a Qualified Trusted Service Provider (QTSP) as defined in Regulation (EU) No 910/2014 and provides qualified trust services and is granted the qualified status by the supervisory body (The Norwegian Nkom). Commfides is CA (Certificate Authority) for Qualified Certificates for electronic Signatures and Qualified Certificates for electronic seals. Commfides do within its scope fulfil and act accordingly to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2. Commfides is audited at least every 24 months by a conformity assessment body to confirm that Commfides as qualified trust service providers and the qualified trust services provided by Commfides fulfil the requirements laid down in REGULATION (EU) No 910/2014. Commfides submit the resulting conformity assessment report to the supervisory body (Nkom). Commfides is listed as a TSP in Nkom list https://tl-norway.no/TSL/NO_TSL.PDF . This list is referred in the "EU Trusted List of Trust Service Providers" here https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.