SUBSCRIBER AGREEMENT (not for SSL certificates)

You are receiving this subscriber agreement because you/your organisation have/has applied for certificates for encrypting and signing e-mails. This subscriber agreement addresses the most important issues which you must observe when using these certificates. For more information about the certificates applied for, please contact the technical contact person at your organisation.

(1) I hereby confirm that

a. all information in the certificate is true in as far as I have knowledge of such information and, in the event that any changes become known to me, that I will automatically make such changes known to the technical contact person of my organisation,
b. the certificate received will not be used until the correctness of the data contained in such certificate has been successfully verified,
c. the certificate or private key, respectively, will be created and used exclusively for the approved purposes and in line with the Certification Practice Statement (CPS), which is available at: https://www.bundesdruckerei.de/de/2833-repository,
d. I alone am responsible for protecting the private key and, if applicable, the revocation password against misuse, loss, disclosure, manipulation or unauthorised use,
e. all necessary measures will be taken to prevent unauthorised use of private keys,
f. the key pair was generated with one of the following algorithms (rsa, dsa, ecdsa-Fp, ecgdsa-Fp, ecdsa-F2m or ecgdsa-F2m) and with a minimum length of 2048 bits for rsa/dsa and of 256 bits for ecc, and
g. the use of private keys will be immediately discontinued as soon as
    i. I become aware that the issuing CA has been compromised,
    ii. the certificate in question is revoked or
    iii. the certificate has reached the end of its validity period.

(2) Furthermore, I hereby warrant that I will no longer use the certificate and the pertinent private key and will request their revocation using the method referred to below as soon as one of the following events occurs:

a. Suspicion or certainty that the private key has been compromised
b. Loss of exclusive control over the private key (e.g. a third party has stolen your PIN)
c. Any changes in certificate data (e. g. name, addresses or affiliation with the organisation).

If you wish to have your certificate revoked, please contact the technical contact person at your organisation.

You can also have your certificate revoked by calling our hotline, however, this is only possible if your organisation has provided you with a revocation password.

- Telephone: + 49 (0) 30 / 25 93 91 - 601

(3) I hereby acknowledge and agree that

a. as part of checking application data, the HR department or my superiors, respectively, or customers may be contacted in order to check the application and the application data with a view to my affiliation with the organisation and/or authorisation as the person responsible for the key,
b. the CSP will save all information from the certificate application and from subsequent authentication, verification and, if applicable, revocation,
c. the CSP generally publishes certificates for certificate status requests, and
d. browser manufacturers, by integrating root certificates of the CSP and the resultant error-message-free use of certificates by subjects, are beneficiary third parties.