AGENCY FOR DIGITAL GOVERNMENT

Den Danske Stat

OCSP Service Integration

Contents

0 Changelog

Date	Version	Change description
23-6-2022	1.0	Initial version

0.1 References

Term	Reference
[CPS]	Certification Practice Statement, Den Danske Stat. https://www.ca1.gov.dk/practice/
[CERTPROF]	Certificate Profiles, Den Danske Stat. https://www.ca1.gov.dk/practice/
[OCES Employee]	Certificate Policy for OCES employee certificates (Public Certificates for Electronic Service). Agency for Digital Government Version 7.1, October 2021. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[OCES Organization]	Certificate Policy for OCES organizational certificates (Public Certificates for Electronic Services). Agency for Digital Government. Version 7.1, October 2021. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Employee]	Certificate Policy for qualified employee certificates. Agency for Digital Government Version 1.1, October 2021. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Organization]	Public Certificate Policy for qualified organizational certificates. Agency for Digital Government. Version 1.1, October 2021. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Person]	Public Certificate for qualified person certificates. Agency for Digital Government Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[RFC6960]	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, Internet Engineering Task Force (IETF), Request for Comments: 6960, June 2013. https://datatracker.ietf.org/doc/html/rfc6960

1 Introduction

Den Danske Stat CA1 is a qualified trust service provider issuing certificate meeting the requirements in the certificate policies [OCES Employee, OCES Organization, Qualified Employee, Qualified Organization and Qualified Person].

For relying parties intending to use the certificates, Den Danske Stat's Certification Practice Statement [CPS], REQ 2.1-05 stipulates requirements on relying parties to ensure, prior to trusting a certificate:

- that the certificate is valid and has not been revoked at the time of the private key usage - i.e. is not listed on the CA's CRL,
- that the purpose for which the certificate is to be used is suitable in respect of any use limitations in the certificate and
- that the use of the certificate in general is suitable in terms of the level of security as described in this applicable certificate policy.

For all subject and subscriber certificates Certificate Profiles [CERTPROF] includes information on how Den Danske Stat CA1 provides certificate revocation information using CRL and OCSP.

This document intends to aid system integrators with guidance information on relevant sections from the [CPS] and [CERTPROF] which may be valuable when integrating with the OCSP services provided by Den Danske Stat CA1.

2 Definitions and abbreviations

Term	Description
PKI System	See [CPS]

3 Introduction to OCSP

Online Certificate Status Protocol (OCSP) provides relying parties with a mechanism to obtain certificate revocation information without checking against Certificate Revocation Lists (CRL). As these lists tend to grow in size, OCSP is often considered the preferred scheme as the request and responses are much smaller. In some use cases, however, it is more optimal to have a scheduled backend retrieval and parsing of CRLs.

While Den Danske Stat CA1 issues new CRLs within one minute after the PKI System has received and approved the revocation request, the revocation status using OCSP as the alternative provides the timely revocation status of the certificate.

The OCSP responder is available through HTTP using the URL: http://ca1.gov.dk/ocsp. The URL is also included in the certificate and can be seen in the Authority Information Access extension.

There is no access control for use of the service.

4 Trusting the OCSP responder

Den Danske Stat's OCSP responder provides revocation information for the certificate hierarchies described in the [CPS]. For all certificates, the OCSP endpoint is the same as the OCSP responder using certificate authority information in the request can figure out if the certificate is a qualified certificate or OCES certificate. In all cases, the OCSP responder uses a certificate from the same certification authority as the certificate which is requested revocation information for. The Certificate Profiles [CERTPROF] describes the OCSP responder certificates for both OCES and Qualified level.

As the OCSP responder certificates are issued by the same certification authority as the subject certificate, trusting the OCSP responder certificates is of similar concern. As part of verifying the OCSP response, the relying party shall also ensure that the OCSP responder certificate can be verified being part of a certificate chain for the applicable certification authority.

5 OCSP profile

The profile for OCSP request and responses follows [RFC6960] and is described in Certificate Profile [CERTPROF].

The Nonce field for OCSP responses contains the value as received in the OCSP request. This also means that if the request does not contain a nonce, the response will likewise also not include a nonce.