

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 25059-2010

**Information security technology -- Public key infrastructure --
Simple online certificate status protocol**

信息安全技术 公钥基础设施 简易在线证书状态协议

(English Translation)

Issued on: September 2, 2010

Implemented on: February 1, 2011

Issued by: Standardization Administration of China

Table of Contents

Introduction

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviations

5 General

5.1 Overview

5.2 Request

Foreword

Appendix A of this standard is an informative annex, Annex B normative appendix.

This standard by the National Safety Standardization Technical Committee (TC260) and focal points.

Drafting of this standard. Shanghai Engineering Research Center for Information Security, National Information Security Engineering Research Center.

Introduction

In many applications based on PKI, there is such a case, an application server system upon completion of its function, the need for A large number of real-time certificate status queries. In this case, the application server certificate status query performance and efficiency requirements ratio Higher, if follow standard OCSP protocol, a protocol data unit complex, signature and verification operations overhead sign makes certificate status Query operation become the bottleneck of application server performance. In the process of practical application, the application servers and OCSP servers often bits the same trusted network or network segment, so as to eliminate this bottleneck, we need to simplify the standard OCSP protocol, solid design Now a lightweight certificate status query protocol.

Information security technology - Public key infrastructure Easy Online Certificate Status Protocol

1 Scope

This standard specifies a simple on-line Certificate Status Protocol --- SOCSP. This protocol can be used as additional criteria OCSP protocol.

This standard describes the following.

- a) detailed description of the request in the form of summary Online Certificate Status Protocol;
- b) detailed description of the response in the form of summary Online Certificate Status Protocol;
- c) Analysis of the various anomalies that may arise when dealing with simple line Certificate Status Protocol responses;
- d) illustrate a simple online certificate status protocol based on the Hypertext Transfer Protocol (HTTP) is applied.

This standard applies to all types of applications and computing environments based on public key infrastructure.

2 Normative references

The following documents contain provisions which, through reference in this standard and become the standard terms. For dated references, subsequent Amendments (not including errata content) or revised edition are not used in this standard, however, encourage the parties to the agreement are based on research Whether the latest versions of these documents. For undated reference documents, the latest versions apply to this standard.

GB/T 19713-2005 Information technology - Security techniques Public Key Infrastructure Online Certificate Status Protocol

3 Terms and Definitions

The following terms and definitions apply to this standard.

Certificate serial number by a certificate authority to generate a unique number corresponding to each certificate.

Hash hash

Maps values from a large (potentially large) domain into a smaller range of (mathematical) algorithm.

Requestor requester

Application subject line certificate status checking services.

Responder

Provides online certificate status inquiry service subject.

4 Abbreviations

The following abbreviations apply to this standard.

CRL certificate revocation list (CertificateRevocationList) DER Distinguished Encoding Rules (DistinguishedEncodingRules) HTTP Hypertext Transfer Protocol (HypertextTransferProtocol) MAC message authentication code (MessageAuthenticationCodes)