# МОНГОЛ УЛСЫН СТАНДАРТ

**Ангилалтын код 2560**

| | |
|---|---|
| **X.509 Интернэтийн нийтийн түлхүүрийн дэд бүтэц Онлайн гэрчилгээний төлөв байдлын протокол – ОГТБП** | **MNS xxxx** |
| **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** | **RFC 2560** |

**Энэ тэмдэглэлийн тухайд**

Энэ баримт бичиг нь интернэтийн стандартыг хянах протоколыг тодорхойлж, түүнийг сайжруулах талаар хэлэлцүүлэг өрнүүлж, зөвлөмж, санал хүсэлтээ ирүүлэхийг интернэтийн нийгэмлэгээс хүссэн. "Интернэтийн албан ёсны протоколын стандартууд" (STD 1) -ын сүүлийн хэвлэлээс энэхүү протоколын стандартчиллын өнөөгийн байдал төлөвийг харна уу.

Энэхүү тэмдэглэлийг цааш нь тарааж түгээхэд ямар нэгэн хязгаарлалт байхгүй.

**Зохиогчийн эрхийн мэдэгдэл**



**1. Оршил**

Энэхүү баримт бичиг нь хүчингүй гэрчилгээний жагсаалт -ХГЖ (CRL) шаардахгүйгээр тоон гэрчилгээний одоогийн төлөв байдлыг тодорхойлоход хэрэгтэй протоколыг зааж өгсөн юм. Нийтийн түлхүүрийн дэд бүтэц X.509-ийн (НТДБХ) үйл ажиллагааны нөхцөл шаардлагыг хангах нэмэлт механизмуудыг тусдаа өөр баримт бичигт тусгасан болно.

Уг протоколын тоймыг 2-р хэсэгт зааж өгсөн. Функциональ шаардлагыг 4-р хэсэгт тодорхойлсон бөгөөд протоколын дэлгэрэнгүйг 5-р хэсэгт үзүүлсэн. Бид протоколын аюулгүй байдлын асуудлыг 6-р хэсэгт тусгасан болно. Хавсралт А нь гипертекст дамжуулах протокол (HTTP) дэх ОГТБП -ийг тодорхойлдог. Хавсралт В нь Хийсвэр синтакс тэмдэглэгээ.1 (XCT.1) (Abstract Syntax Notation One-ASN.1)- ийн синтаксийн элементүүдийг багтаасан ба хавсралт С нь мессежний “Олон зориулалттай интернэт шуудангийн өргөтгөлүүд -(Multipurpose Internet Mail Extensions (MIME) )” төрлийг тодорхойлсон болно.

Энэхүү баримт бичигт "ёстой (MUST)", "ёсгүй (MUST NOT)", "шаардлагатай (REQUIRED)", “ байх болно(SHALL)", "болохгүй(SHALL NOT)"," байх ёстой-(SHOULD)", " байх ёсгүй-(SHOULD NOT)", "зөвлөмж болгосон (RECOMMENDED)", "болох (MAY)", "сонголттой (OPTIONAL)" гэсэн (том үсгээр харуулсан байгаа) түлхүүр үгсийг энэхүү баримт бичигт (RFC2119) –д [Request For Comments - Internet X.509 Public Key Infrastructure Certificate and CRL Profile]тодорхойлсны дагуу тайлбарлах нь зүйтэй.

**2. Протоколын тойм**

ХГЖ-ийг тогтсон хугацаанд байнга шалгахын оронд эсвэл гэрчилгээг хүчингүй болгосон байдлын талаарх мэдээллийг цаг тухайд нь нэмэлтээр авах шаардлагатай байж болно ([RFC2459], 3.3-р хэсгийг үзнэ үү). Тухайлбал, өндөр дүнтэй хөрөнгийн шилжүүлэг эсвэл томоохон хувьцааны арилжаа байж болно.

Онлайн гэрчилгээний төлөв байдлын протокол – ОГТБП нь тодорхой заасан гэрчилгээний (хүчингүй болгосон) төлөв байдлыг тодорхойлохын тулд хэрэглээний программуудыг ашиглах

боломжийг олгодог. ОГТБП -ийг ХГЖ-аас илүүтэйгээр хүчингүй болгох мэдээллийг цаг тухайд нь өгөх үйл ажиллагааны зарим шаардлагыг хангахын тулд ашиглаж болох ба төлөв байдлын нэмэлт мэдээлэл авахад ашиглаж болно. ОГТБП үйлчлүүлэгч нь ОГТБП хариулагч руу төлөв байдлын хүсэлт гаргаж, хариулагч хариу өгөх хүртэл тухайн гэрчилгээг хүлээн авахыг түдгэлзүүлдэг.

Энэ протокол нь гэрчилгээний төлөв байдлыг шалгаж буй программ болон тухайн төлөв байдлыг өгч буй серверийн хооронд солилцох шаардлагатай өгөгдлийг тодорхойлдог.

**2.1 Хүсэлт**

ОГТБП - хүсэлт нь дараах өгөгдлийг агуулдаг. Үүнд:

- протоколын хувилбар
- үйлчилгээний хүсэлт
- зорилтот гэрчилгээ танигч
- ОГТБП-хариулагчаар боловсруулж БОЛОХ сонголтын өргөтгөлүүд.

Хүсэлтийг хүлээн авсны дараа ОГТБП хариулагч нь дараах тохиолдолд дараах байдлаар тодорхойлно. Үүнд:

1. Мэдээ сайн бүрдсэн байна
2. Хариулагч нь хүсэлт гаргасан үйлчилгээг үзүүлэхээр тохируулсан ба
3. Хүсэлт нь хариулагчийн шаардлагатай мэдээллийг агуулах ба хэрэв өмнөх нөхцөлүүдийн аль нэг нь хангагдаагүй бол ОГТБП хариулагч алдааны мэдэгдэл гаргадаг; эс бөгөөс энэ нь тодорхой хариултыг буцаана.

**2.2 Хариулт**

ОГТБП хариултууд нь янз бүрийн хэлбэртэй байж болно. ОГТБП хариулт нь хариултын төрөл ба бодит хариултын байтуудаас бүрдэнэ. Бүх ОГТБП серверүүд болон үйлчлүүлэгчид дэмжих ёстой ОГТБП хариултын нэг үндсэн төрөл байдаг. Энэ хэсгийн үлдсэн хэсэг нь зөвхөн энэ үндсэн хариултын төрөлд хамаарна.

Бүх тодорхой хариу мессежнүүд тоон гарын үсэгтэй байна. Хариултад гарын үсэг зурахад ашигласан түлхүүр нь дараах зүйлсийн аль нэгэнд хамаарах ёстой.Үүнд:

- тухайн гэрчилгээ олгосон гэрчилгээ олгох эрх бүхий байгууллага
- нийтийн түлхүүр нь хүсэлт гаргагч талд итгэмжлэгдсэн найдвартай (итгэгдсэн) хариулагч
- Хариуцагч нь гэрчилгээжүүлэх байгууллага (ГБ)-д ОГТБП-ийн хариултыг гаргаж болно гэдгийг харуулсан, ГБ-аас шууд олгосон тусгайлан тэмдэглэсэн гэрчилгээтэй ГБ-ийн томилсон хариулагч (эрх бүхий хариулагч)

Тодорхой хариу мессеж нь дараах зүйлээс бүрдэнэ:

- хариултын синтаксийн хувилбар
- хариулагчийн нэр
- гэрчилгээ тус бүрийн хүсэлтийн хариулт
- нэмэлт өргөтгөлүүд
- объект танигч гарын үсгийн алгоритм (object identifiers- OID)
- хариултын хэш дээр тооцоолсон гарын үсэг

Хүсэлтэд байгаа гэрчилгээ бүрийн хариу нь дараах зүйлээс бүрдэнэ:

- зорилтот гэрчилгээг танигч
- гэрчилгээний төлөв байдлын утга
- хариултын хүчинтэй хугацааны интервал

- нэмэлт сонголттой өргөтгөлүүд

Энэ стандарт нь дараах эцсийн хариуг тодорхойлдог гэрчилгээний төлөв байдлын утгыг ашиглах үзүүлэлтүүдтэй. Эдгээр нь:

- Сайн
- хүчингүй болгосон
- үл мэдэгдэх

"Сайн" төлөв байдал нь статусын лавлагаанд эерэг хариу ирснийг илтгэнэ. Хамгийн багадаа энэхүү эерэг хариу нь гэрчилгээг хүчингүй болгоогүйг илтгэж байгаа боловч гэрчилгээ хэзээ нэгэн цагт олгогдсон эсвэл хариу өгөх хугацаа нь гэрчилгээний хүчинтэй байх хугацаанд байна гэсэн үг биш юм. Хариултын өргөтгөлүүдийг гэрчилгээ олгох, хүчинтэй байх гэх мэт эерэг мэдэгдэл гэрчилгээний статусын талаар хариулагчийн хийсэн мэдэгдлийн талаар нэмэлт мэдээллийг дамжуулахад ашиглаж болно.

"Хүчингүй болсон" төлөв нь гэрчилгээг хүчингүй болгосон (бүрмөсөн эсвэл түр хугацаагаар (түр саатсан)) байгааг харуулж байна.

"Үл мэдэгдэх" байдал нь хариулагч нь хүсэлт гаргасан гэрчилгээний талаар мэдэхгүй байгааг илтгэнэ.

**2.3 Онцгой тохиолдлууд**

Алдаа гарсан тохиолдолд ОГТБП хариулагч алдааны мессежийг буцаана. Эдгээр зурвасуудад гарын үсэг зураагүй байна. Алдаа нь дараах төрлийн байж болно.

- алдаатай хүсэлт
- дотоод алдаа
- дараа дахин оролдоно уу
- гарын үсэг шаардлагатай
- зөвшөөрөлгүй

Хүлээн авсан хүсэлт нь ОГТБП-ийн синтакстай нийцэхгүй байвал сервер нь "алдаатай хүсэлт" (malformed Request) гэсэн хариултыг гаргадаг.

"Дотоод алдаа" гэсэн хариулт нь ОГТБП хариулагч дотоод зөрчилтэй байдалд хүрсэн болохыг харуулж байна. Асуулгыг өөр хариулагчтай дахин оролдох шаардлагатай. ОГТБП хариулагч ажиллаж байгаа боловч хүссэн гэрчилгээний төлөвийг буцааж мэдүүлэх боломжгүй тохиолдолд эсвэл түр хугацаанд хариу өгөх боломжгүй гэдгийг "Дараа дахин оролдоно уу" гэсэн хариултыг ашиглаж болно. "Гарын үсэг шаардлагатай" гэсэн хариултыг сервер хариу бичихийн тулд үйлчлүүлэгчээс хүсэлтэд гарын үсэг зурахыг шаардсан тохиолдолд буцаана. Үйлчлүүлэгч энэ серверт энэ асуулга хийх эрхгүй тохиолдолд "зөвшөөрөлгүй" гэсэн хариултыг буцаана.

**2.4 “Энэ шинэчлэлт, дараагийн шинэчлэлт болон энд үйлдвэрлэсэн” гэдгийн семантик – (thisUpdate, nextUpdate болон producedAt)**

Хариултууд нь “thisUpdate, nextUpdate болон productionAt”-ыг гурван удаа агуулж болно. Эдгээр талбаруудын семантик нь:

- thisUpdate: Заасан төлөв байдал зөв болох нь мэдэгдэж байгаа цаг
- NextUpdate: Гэрчилгээний төлөв байдлын талаар шинэ мэдээлэл гарах эсвэл түүнээс өмнө гарах цаг
- producedAt: ОГТБП хариулагч энэ хариуд гарын үсэг зурсан цаг.

Хэрэв NextUpdate тохируулагдаагүй бол хариулагч нь хүчингүй болгох тухай шинэ мэдээлэл байнга бэлэн байгааг харуулж байна.

### 2.5 Хариулт- Урьдчилсан үйлдвэрлэл (Response Pre-production)

ОГТБП хариулагч нар тодорхой хугацаанд гэрчилгээний төлөв байдлыг тодорхойлсон гарын үсэг бүхий хариуг урьдчилан гаргаж болно. Тухайн төлөв байдал зөв гэж мэдэгдэж байсан цагийг хариултын thisUpdate талбарт тусгана. nextUpdate талбарт шинэ мэдээлэл гарах эсвэл түүнээс өмнөх цагийг тусгах бол хариу гарсан цаг нь хариултын productionAt талбарт харагдана.

### 2.6 ОГТБП гарын үсэг зурах эрх бүхий төлөөлөгч

Гэрчилгээний төлөвийн мэдээлэлд гарын үсэг зурдаг түлхүүр нь гэрчилгээнд гарын үсэг зурсан түлхүүр байх албагүй. Сертификат гаргагч нь ОГТБП гарын үсэг зурагчийн гэрчилгээнд extendedKeyUsage-д зориулсан өвөрмөц утгыг агуулсан гэрчилгээ олгох замаар ОГТБП -д гарын үсэг зурах эрхийг шууд шилжүүлдэг. Энэхүү гэрчилгээг хүлээн авагч Гэрчилгээжүүлэх байгууллагаас (ГБ) шууд хариуцагчид өгөх ёстой.

### 2.7 ГБ -ийн түлхүүрийг тохиролцох

Хэрэв ОГТБП хариулагч тодорхой ГБ -ийн хувийн түлхүүр алдагдсаныг мэдэж байгаа бол тухайн ГБ -аас олгосон бүх гэрчилгээний хүчингүй болсон төлөв байдлыг буцаан өгч болно.

## 3. Үйл ажиллагааны шаардлага

### 3.1 Гэрчилгээний агуулга

ОГТБП -ийн үйлчлүүлэгчдэд мэдээллийн хүртээмжийн сайн мэддэг цэгийг дамжуулахын тулд ГБ-ууд нь AuthorityInfoAccess өргөтгөлийг ([RFC2459], 4.2.2.1-д тодорхойлсон) ОГТБП ашиглан шалгаж болох гэрчилгээнд оруулах боломжийг олгоно. Эсвэл ОГТБП үйлчилгээ үзүүлэгчийн хандалтын байршлыг ОГТБП үйлчлүүлэгч дээр дотооддоо тохируулж болно.

Локал байршуулсан эсвэл эрх бүхий хариулагчийн өгсөн ОГТБП үйлчилгээг дэмждэг ГБ-ууд AccessDescription SEQUENCE-д accessMethod-д зориулсан uniformResourceIndicator (URI) байршлын утга болон OID утгын id-ad-ocsp-ийг оруулах ёстой.

Тухайн гэрчилгээ дэх accessLocation талбарын утга нь ОГТБП хариулагч руу хандахад ашигладаг тээвэрлэлтийг (жишээ нь HTTP) тодорхойлдог ба мөн тээвэрлэлтээс хамааралтай бусад мэдээллийг (жишээ нь URL) агуулж болно.

### 3.2 Гарын үсэг зурсан хариу хүлээж авах шаардлага

Гарын үсэг зурсан хариуг хүчинтэй гэж хүлээн зөвшөөрөхөөс өмнө ОГТБП үйлчлүүлэгчид дараах зүйлийг баталгаажуулах ёстой. Үүнд:

1. Хүлээн авсан хариуд тодорхойлсон гэрчилгээ нь холбогдох хүсэлтэд тодорхойлсон гэрчилгээтэй тохирч байгаа;
2. Хариулт дээрх гарын үсэг хүчинтэй;
3. Гарын үсэг зурсан хүний хувийн мэдээлэл нь хүсэлтийг хүлээн авагчтай таарч байна.
4. Гарын үсэг зурсан хүн хариуд гарын үсэг зурах эрхтэй.
5. Заасан төлөв байдал нь зөв гэж мэдэгдэж байгаа цаг хугацаа (thisUpdate) хангалттай саяхан байна.
6. Боломжтой үед гэрчилгээний төлөв байдлын талаар шинэ мэдээлэл гарах эсвэл түүнээс өмнө (nextUpdate) хугацаа нь одоогийн хугацаанаас их байна.

## 4. Нарийвчилсан протокол

Хийсвэр синтакс тэмдэглэгээ.1 (XCT.1) (ASN.1) синтакс нь [RFC2459]-д тодорхойлсон нэр томьёог авч ашигладаг. Гарын үсгийн тооцооллын хувьд гарын үсэг зурах өгөгдлийг Хийсвэр синтакс тэмдэглэгээ.1 онцолж ялгасан кодчиллын дүрмүүдийг (DER) [X.690] ашиглан кодчилдог.

Хийсвэр синтакс тэмдэглэгээ.1 EXPLICIT шошго нь өөрөөр заагаагүй бол анхдагч байдлаар ашиглагддаг.

Өөр газраас импортолсон нэр томьёо нь: Өргөтгөл, Сертификатын серийн дугаар, Тухайн нийтийн түлхүүрийн мэдээлэл, Нэр, Алгоритм танигч, ХГЖ-ийн шалтгаан

### 4.1 Хүсэлтүүд

Энэ хэсэгт баталгаажуулах хүсэлтийн Хийсвэр синтакс тэмдэглэгээ.1 тодорхойлолтыг зааж өгсөн болно. Мессежний бодит формат нь ашигласан тээвэрлэлтийн механизмаас (HTTP, SMTP, LDAP гэх мэт) хамаарч өөр өөр байж болно.

#### 4.1.1 Хүсэлтийн синтакс

```
OCSPRequest ::=          SEQUENCE {
        tbsRequest                  TBSRequest,
        optionalSignature [0] EXPLICIT Signature OPTIONAL }
TBSRequest ::=           SEQUENCE {

        version                 [0]  EXPLICIT Version DEFAULT v1,
        requestorName       [1]  EXPLICIT GeneralName OPTIONAL,
        requestList                 SEQUENCE OF Request,
        requestExtensions [2] EXPLICIT Extensions OPTIONAL }
Signature ::=                SEQUENCE {
        signatureAlgorithm   AlgorithmIdentifier,
        signature                   BIT STRING,
        certs                       [0] EXPLICIT SEQUENCE OF Certificate
OPTIONAL}

Version         ::=                 INTEGER { v1(0) }

Request         ::=          SEQUENCE {
        reqCert CertID,
        singleRequestExtensions [0] EXPLICIT Extensions OPTIONAL }

CertID          ::=          SEQUENCE {
        hashAlgorithm     AlgorithmIdentifier,
        issuerNameHash    OCTET STRING, -- Hash of Issuer's DN
        issuerKeyHash     OCTET STRING, -- Hash of Issuers public key
        serialNumber      CertificateSerialNumber }
```

Энд issuerNameHash нь үүсгэгчийн онцгой нэрийн хэш юм. Хэшийг шалгаж буй гэрчилгээнд үүсгэгчийн нэрийн талбарын DER кодчиллоор тооцно. issuerKeyHash нь Үнэт цаас гаргагчийн нийтийн түлхүүрийн хэш юм. Хэшийг гаргагчийн гэрчилгээний тухайн нийтийн түлхүүрийн талбарын утга (шошго ба уртаас бусад) дээр тооцно. Эдгээр хэшийн аль алинд нь ашигладаг хэш алгоритмыг hashAlgorithm-д тодорхойлсон бөгөөд серийн дугаар нь төлөвийг хүссэн гэрчилгээний серийн дугаар юм.

#### 4.1.2 Хүсэлтийн синтаксийн талаарх тэмдэглэл

Үүсгэгчийг тодорхойлохын тулд ГБ-ийн нэрийн хэшээс гадна ГБ-ийн нийтийн түлхүүрийн хэшийг ашиглах үндсэн шалтгаан нь хоёр ГБ ижил нэрийг ашиглах боломжтой байж болох юм (Энэ Нэрийн өвөрмөц байдал нь үүнийг хэрэгжүүлэх боломжгүй гэсэн зөвлөмж өгч байна).

Гэсэн хэдий ч ГБ-ууд хувийн түлхүүрээ хуваалцахаар шийдээгүй эсвэл аль нэг ГБ-ын түлхүүр алдагдаагүй л бол хоёр ГБ хэзээ ч ижил нийтийн түлхүүртэй байдаггүй.

Аливаа тусгай өргөтгөлийн дэмжлэгийг ЗААВАЛ хийх албагүй. Тэдний алинд нь ч эгзэгтэй гэсэн тэмдэг тавьж болохгүй. 4.4-т хэд хэдэн ашигтай өргөтгөлүүдийг санал болгосон байгаа. Нэмэлт өргөтгөлүүдийг нэмэлт “Request For Comments” (RFC)-д тодорхойлж болно. Танигдаагүй өргөтгөлүүдийг орхих ёстой (хэрэв тэдгээр нь чухал тэмдэг тавиагүй бөгөөд ойлгомжгүй бол).

Хүсэлт гаргагч нь ОГТБП хүсэлтэд гарын үсэг зурж болно. Энэ тохиолдолд гарын үсгийг tbsRequest бүтэц дээр тооцоолно. Хэрэв хүсэлтэд гарын үсэг зурсан бол хүсэлт гаргагч нь хүсэлт гаргагчийн нэр талбарт нэрээ зааж өгнө. Мөн гарын үсэг зурсан хүсэлтийн хувьд хүсэлт гаргагч нь ОГТБП -ийн хариулагчийн гарын үсгийн гэрчилгээний талбарт хүсэлт гаргагчийн гарын үсгийг баталгаажуулахад туслах гэрчилгээг оруулж болно.

### 4.2 Хариултын синтакс

Энэ хэсэг нь баталгаажуулах хариултын ХСТ.1 тодорхойлолтыг зааж өгсөн. Мессежний бодит формат нь ашигласан тээвэрлэлтийн механизмаас (HTTP, SMTP, LDAP гэх мэт) хамаарч өөр өөр байж болно.

#### 4.2.1 ОГТБП хариултын ХСТ.1-ийн тодорхойлолт

Хамгийн багадаа ОГТБП -ийн хариулт нь өмнөх хүсэлтийн боловсруулалтын төлөвийг харуулсан хариу нөхцөлийн талбараас бүрдэнэ. Хэрэв respondStatus-ийн утга нь алдааны нөхцөлүүдийн нэг бол respondBytes-г тохируулахгүй.

```
OCSPResponse  ::=  SEQUENCE {
        responseStatus          OCSPResponseStatus,
        responseBytes           [0] EXPLICIT ResponseBytes OPTIONAL }

OCSPResponseStatus  ::= ENUMERATED {
        successful                (0), --Response has valid confirmations
        malformedRequest          (1), --Illegal confirmation request
        internalError             (2), --Internal error in issuer
        tryLater                  (3), --Try again later
                                       --(4) is not used
        sigRequired               (5), --Must sign the request
        unauthorized              (6) --Request unauthorized

}
```

ResponsiveBytes-ын утга нь OCTET STRING гэж кодлогдсон OID-ээр тодорхойлогдсон ОБЪЕКТ ТАНИГЧ болон хариултын синтаксаас бүрдэнэ.

```
ResponseBytes ::=         SEQUENCE {
        responseType   OBJECT IDENTIFIER,
        response          OCTET STRING }
```

Үндсэн ОГТБП хариулагчийн хувьд responceType нь id-pkix-ocsp-basic байх болно.

```
id-pkix-ocsp          OBJECT IDENTIFIER ::= { id-ad-ocsp }
id-pkix-ocsp-basic    OBJECT IDENTIFIER ::= { id-pkix-ocsp 1 }
```

ОГТБП хариулагч нь idpkix-ocsp-basic төрлийн хариу өгөх чадвартай байх ёстой. Үүний дагуу ОГТБП үйлчлүүлэгчид нь id pkix-ocspbasic төрлийн хариултыг хүлээн авч, боловсруулах чадвартай байх ёстой.

Хариултын утга нь BasicOCSPResponse-ийн DER кодчилол байх ёстой.

```
BasicOCSPResponse       ::= SEQUENCE {
        tbsResponseData      ResponseData,
```

```
        signatureAlgorithm   AlgorithmIdentifier,
        signature            BIT STRING,
        certs               [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }
```

Гарын үсгийн утгыг ResponseData кодчиллын DER-ийн хэш дээр тооцно.

```
ResponseData  ::= SEQUENCE {
        version            [0] EXPLICIT Version DEFAULT v1,
        responderID             ResponderID,
        producedAt              GeneralizedTime,
        responses              SEQUENCE OF SingleResponse,
        responseExtensions  [1] EXPLICIT Extensions OPTIONAL }
ResponderID ::= CHOICE {
        byName [1] Name,
        byKey [2] KeyHash }

KeyHash ::= OCTET STRING -- SHA-1 hash of responder's public key
(excluding the tag and length fields)

SingleResponse ::= SEQUENCE {
        certID                  CertID,
        certStatus               CertStatus,
        thisUpdate               GeneralizedTime,
        nextUpdate        [0]    EXPLICIT GeneralizedTime OPTIONAL,
        singleExtensions  [1]    EXPLICIT Extensions OPTIONAL }

CertStatus ::= CHOICE {
        good      [0]      IMPLICIT NULL,
        revoked   [1]      IMPLICIT RevokedInfo,
        unknown   [2]      IMPLICIT UnknownInfo }

RevokedInfo ::=  SEQUENCE {
        revocationTime           GeneralizedTime,
        revocationReason   [0]   EXPLICIT CRLReason OPTIONAL }

UnknownInfo ::= NULL -- this can be replaced with an enumeration
```

### 4.2.2 ОГТБП хариултын талаарх тэмдэглэл

#### 4.2.2.1 Хугацаа

ThisUpdate болон nextUpdate талбарууд нь санал болгож буй хүчинтэй байх интервалыг тодорхойлдог. Энэ интервал нь ХГЖ-ын {thisUpdate, nextUpdate} интервалтай тохирч байна. Дараагийн шинэчлэлтийн утга нь дотоод системийн цагийн утгаас өмнөх хариултуудыг найдваргүй гэж үзэх хэрэгтэй. ThisUpdate хугацаа нь дотоод системийн цагаас хожимдсон хариултуудыг найдваргүй гэж үзэх хэрэгтэй. NextUpdate утгыг тохируулаагүй хариултууд нь NextUpdate хийх хугацаагүй ХГЖ-тай адил байна (2.4-р хэсгийг үзнэ үү). producedAt цаг нь энэ хариуд гарын үсэг зурсан цаг юм.

#### 4.2.2.2 Эрх бүхий хариулагч

Гэрчилгээний төлөв байдлын мэдээлэлд гарын үсэг зурах түлхүүр нь гэрчилгээнд гарын үсэг зурсан түлхүүр байх албагүй. Гэсэн хэдий ч энэ мэдээлэлд гарын үсэг зурсан байгууллага үүнийг хийх эрхтэй эсэхийг баталгаажуулах шаардлагатай. Тиймээс гэрчилгээ гаргагч нь ОГТБП -ийн хариуд өөрөө гарын үсэг зурах эсвэл энэ эрх мэдлийг өөр байгууллагад тодорхой зааж өгөх ёстой. ОГТБП гарын үсэг зурах төлөөлөгчийг ОГТБП хариултын гарын үсэг зурсан гэрчилгээнд орсон өргөтгөсөн түлхүүрийн ашиглалтын гэрчилгээний өргөтгөлд id-kp-OCSPSigning оруулснаар томилогдох ёстой. Энэхүү гэрчилгээг тухайн гэрчилгээг олгосон ГБ-аас шууд олгох ёстой.

id-kp-OCSPSigning OBJECT IDENTIFIER ::= {id-kp 9}

ОГТБП -ийн хариулт дээр тулгуурласан систем эсвэл хэрэглээний программууд нь дээр дурдсанчлан id-ad-ocspSigning утгыг илрүүлж, ашиглах чадвартай байх ёстой. Тэд нэг буюу хэд хэдэн ОГТБП гарын үсэг зурах эрх бүхий байгууллагыг дотооддоо тохируулга хийх, гарын үсэг зурсан эрх бүхий байгууллагад итгэмжлэгдсэн ГБ-ийн багцыг зааж өгөх арга хэрэгслээр хангаж болно. Хариулт дээрх гарын үсгийг баталгаажуулахад шаардагдах гэрчилгээ нь дараах шалгууруудаас дор хаяж нэг шалгуурыг хангаагүй тохиолдолд хариу өгөхөөс татгалзах ёстой. Үүнд:

1. Тухайн гэрчилгээний ОГТБП гарын үсэг зурах эрх бүхий локал тохиргоотой таарч байна; эсвэл
2. Тухайн гэрчилгээг олгосон ГБ-ын гэрчилгээ мөн үү; эсвэл
3. ExtendedKeyUsage өргөтгөл дэх id-ad-ocspSigning-ийн утгыг багтаасан бөгөөд тухайн гэрчилгээг олгосон ГБ-аас гаргасан бол

Хүлээн авах эсвэл татгалзах нэмэлт шалгуур нь хариултад өөрт нь эсвэл хариу дээрх гарын үсгийг баталгаажуулахад ашигласан гэрчилгээнд хамаарна.

#### 4.2.2.2.1 Эрх бүхий хариулагчийг хүчингүй болгосон эсэхийг шалгах

Эрх бүхий ОГТБП хариулагч нь нэг буюу хэд хэдэн ГБ-ийн төлөвийн мэдээллийг өгдөг тул ОГТБП -ийн үйлчлүүлэгчид эрх бүхий хариулагчийн гэрчилгээг хүчингүй болгоогүй эсэхийг хэрхэн шалгахыг мэдэх хэрэгтэй. ГБ нь энэ асуудлыг дараах гурван аргын аль нэгээр шийдэж болно. Үүнд:

- ГБ нь ОГТБП үйлчлүүлэгч хариулагчийн гэрчилгээний бүх хугацаанд хариулагчид итгэж болно гэж зааж өгч болно. ГБ нь id-pkix-ocsp-nocheck өргөтгөлийг оруулснаар үүнийг хийдэг. Энэ нь чухал биш өргөтгөл байх ёстой бөгөөд өргөтгөлийн утга NULL байх ёстой. Ийм гэрчилгээ олгож буй ГБ-ууд хариулагчийн түлхүүрийн эвдрэл нь ХГЖ-д гарын үсэг зурахад ашигладаг ГБ түлхүүрийн эвдрэлтэй адил ноцтой гэдгийг наад зах нь энэхүү гэрчилгээний хүчинтэй байх хугацаанд ойлгох ёстой. ГБ-ууд энэ төрлийн гэрчилгээг маш богино хугацаанд олгож, байнга шинэчилж болно.

id-pkix-ocsp-nocheck OBJECT IDENTIFIER ::= { id-pkix-ocsp 5 }

- ГБ нь хариулагчийн гэрчилгээг хүчингүй болгох эсэхийг хэрхэн шалгахыг зааж өгч болно. Хэрэв шалгалтыг ХГЖ эсвэл ХГЖ түгээх цэг ашиглан хийх шаардлагатай бол ХГЖ түгээх цэгийг, хэрэв шалгалтыг өөр аргаар хийх шаардлагатай бол эрх бүхий байгууллагын мэдээллийн хандалтыг ашиглан хийж болно. Эдгээр хоёр механизмын аль нэгийг тодорхойлох дэлгэрэнгүй мэдээллийг [RFC2459]-аас авах боломжтой.
- ГБ нь хариулагчийн гэрчилгээг хүчингүй болгох эсэхийг шалгах ямар нэгэн аргыг зааж өгөхгүй байж болох бөгөөд энэ тохиолдолд тухайн гэрчилгээг хүчингүй болгох эсэхийг шалгах эсэх нь ОГТБП үйлчлүүлэгчийн өөрийнх нь аюулгүй байдлын бодлогоос хамаарна.

### 4.3 Заавал эсвэл сонголтоор хэрэглэх криптографийн алгоритмууд

ОГТБП үйлчилгээ авахыг хүссэн үйлчлүүлэгчид нь [RFC2459]-ийн 7.2.2-т заасан өгөгдлийн бүтэц, алгоритмуудаар (ӨБА) (data structures and algorithms- DSA) *sig-alg-oid*-оор тодорхойлсон ӨБА түлхүүрээр гарын үсэг зурсан хариултуудыг боловсруулах чадвартай байх ёстой. Үйлчлүүлэгчид [RFC2459]-ийн 7.2.1-д заасны дагуу РША-ын (Ривест-Шамир-Адлеман) [RSA -(Rivest–Shamir–Adleman) is a public-key cryptosystem] гарын үсгийг боловсруулах чадвартай байх ёстой. ОГТБП хариулагч нар SHA1 хэш алгоритмыг дэмжих ёстой.

### 4.4 Өргөтгөлүүд

Энэ хэсэг нь X.509-ын 3-р хувилбарын гэрчилгээнд ашигласан өргөтгөлийн загварт үндэслэн зарим стандарт өргөтгөлүүдийг тодорхойлдог [RFC2459]. Бүх өргөтгөлийг дэмжих нь үйлчлүүлэгч болон хариулагчдын аль алинд нь сонголтоор өгөгдөнө.

Өргөтгөл бүрийн хувьд тодорхойлолт нь түүний синтакс, ОГТБП -хариулагчийн гүйцэтгэсэн боловсруулалт болон харгалзах хариултад багтсан өргөтгөлүүдийг заана.

### 4.4.1 Nonce

Nonce *[Криптографийн хувьд nonce гэдэг нь криптограф харилцаанд нэг л удаа ашиглагдах дурын тоо юм. Энэ нь ихэвчлэн санамсаргүй эсвэл псевдо-санамсаргүй тоогоор баталгаажуулах протоколд гаргаж өгдөг бөгөөд дахин давтах халдлагад өмнөх харилцааг дахин ашиглах боломжгүй болгоно.]* нь дахин давтах халдлагаас сэргийлэхийн тулд хүсэлт болон хариуг криптограф аргаар холбож өгдөг. Nonce нь хүсэлтийн хувьд хүсэлтийн өргөтгөлүүдийн (requestExtensions) нэг бөгөөд хариултуудын хувьд хариу өргөтгөлүүдийн (responseExtensions) нэгд багтдаг. Хүсэлт болон хариултын аль алинд нь nonce нь id-pkix-ocsp nonce объект танигчаар тодорхойлогддог бөгөөд extnValue нь nonce-ийн утга юм.

id-pkix-ocsp-nonce OBJECT IDENTIFIER ::= { id-pkix-ocsp 2 }

### 4.4.2 ХГЖ лавлагаа

ОГТБП хариулагч хүчингүй болсон эсвэл хүлээгдэж буй (onHold) гэрчилгээ олдсон ХГЖ-г зааж өгөх нь зүйтэй. Энэ нь ОГТБП -ийг агуулахуудын хооронд ашиглах, мөн аудитын механизм болгон ашиглахад хэрэг болно. ХГЖ-ийг URL (ХГЖ-г ашиглах боломжтой URL), тоо (ХГЖ дугаар) эсвэл цаг (холбогдох ХГЖ үүсгэсэн цаг) зааж өгч болно. Эдгээр өргөтгөлүүдийг singleExtensions гэж зааж өгөх болно. Энэ өргөтгөлийн танигч нь id-pkixocsp-crl байх ба утга нь CrlID байх болно.

id-pkix-ocsp-crl OBJECT IDENTIFIER ::= { id-pkix-ocsp 3 }

```
CrlID  ::=  SEQUENCE {
        crlUrl          [0] EXPLICIT IA5String OPTIONAL,
        crlNum          [1] EXPLICIT INTEGER OPTIONAL,
        crlTime         [2] EXPLICIT GeneralizedTime OPTIONAL }
```

crlUrl сонголтын хувьд IA5String нь ХГЖ боломжтой URL-г зааж өгнө. crlNum-ийн хувьд INTEGER нь холбогдох ХГЖ-ийн ХГЖ дугаарын өргөтгөлийн утгыг зааж өгнө. crlTime-ийн хувьд Ерөнхий цаг (GeneralizedTime) нь холбогдох CRL гарсан цагийг заана.

### 4.4.3 Зөвшөөрөгдөх хариултын төрлүүд

ОГТБП -ийн үйлчлүүлэгч өөрийн ойлгож буй хариултын төрлийг зааж өгөхийг хүсэж болно. Үүнийг хийхийн тулд объект танигч idpkix-ocsp-response болон AcceptableResponses утга бүхий өргөтгөлийг ашиглах ХЭРЭГТЭЙ. Энэ өргөтгөл нь хүсэлтийн өргөтгөлүүдийн нэг болгон орсон болно. AcceptableResponses-д багтсан объект танигч нь энэ үйлчлүүлэгчийн хүлээн авах боломжтой янз бүрийн хариултын объект танигчууд юм (жишээ нь, id-pkix-ocsp-basic).

id-pkix-ocsp-response OBJECT IDENTIFIER ::= { id-pkix-ocsp 4 }

AcceptableResponses ::= SEQUENCE OF OBJECT IDENTIFIER

4.2.1-д дурдсанчлан ОГТБП хариулагч нь id-pkix-ocsp-үндсэн хариултын төрлөөр хариулах чадвартай байх ёстой. Үүний дагуу ОГТБП үйлчлүүлэгчид id-pkix-ocsp-үндсэн хариултын төрлийн хариуг хүлээн авч, боловсруулах чадвартай байх ёстой.

### 4.4.4 Архивын тасалдал

ОГТБП хариулагч нь гэрчилгээний хугацаа дууссанаас хойш хүчингүй болгох мэдээллийг хадгалахаар сонгож болно. Хариултад гарсан хугацаанаас хадгалалтын интервалын утгыг хассанаар олж авсан огноог гэрчилгээний "архивыг таслах" огноо гэж тодорхойлдог.

ОГТБП -ийг идэвхжүүлсэн программууд нь гарын үсгийг баталгаажуулахад шаардлагатай гэрчилгээний хугацаа аль хэдийн дууссан байсан ч тоон гарын үсгийг үйлдвэрлэсэн өдрөө

найдвартай (эсвэл тийм биш байсан) нотлоход хувь нэмрээ оруулахын тулд ОГТБП архивын тасалдсан огноог ашиглана.

Ийм түүхэн лавлагаанд дэмжлэг үзүүлдэг ОГТБП серверүүд хариултуудад архивын тасалбарын огнооны өргөтгөлийг оруулах ёстой. Хэрэв оруулсан бол энэ утгыг id-pkix-ocsp-archive-cutoff болон GeneralizedTime синтаксоор тодорхойлсон ОГТБП singleExtensions өргөтгөл болгон өгөх ёстой.

id-pkix-ocsp-archive-cutoff OBJECT IDENTIFIER ::= { id-pkix-ocsp 6 }

ArchiveCutoff ::= GeneralizedTime

Жишээлбэл, хэрэв сервер нь 7 жилийн хадгалах интервалын бодлогын хүрээнд ажиллаж, төлөв нь t1 үед үүссэн бол хариулт дахь ArchiveCutoff-ын утга (t1 - 7 жил) байх болно.

### 4.4.5 ХГЖ нэвтрэх өргөтгөлүүд

[RFC2459]-ийн 5.3-р хэсэгт ХГЖ-ийн Entry Extensions гэж заасан бүх өргөтгөлүүдийг мөн singleExtensions хэлбэрээр дэмждэг.

### 4.4.6 Үйлчилгээний байршил тогтоогч

ОГТБП сервер нь хүсэлтийг хүлээн авч, тодорхойлогдсон гэрчилгээ авах эрх мэдэлтэй гэж мэдэгдэж байгаа ОГТБП сервер рүү замчлах маягаар ажиллаж болно. Үйлчилгээний байршил тогтоогч (serviceLocator) хүсэлтийн өргөтгөлийг энэ зорилгоор тодорхойлсон. Энэ өргөтгөл нь хүсэлтийн singleRequestExtension-ийн нэг болгон орсон болно.

id-pkix-ocsp-service-locator OBJECT IDENTIFIER ::= { id-pkix-ocsp 7 }

```
ServiceLocator  ::= SEQUENCE {
        issuer    Name,
        locator   AuthorityInfoAccessSyntax OPTIONAL }
```

Эдгээр талбаруудын утгыг авч үзэж буй гэрчилгээний харгалзах талбаруудаас авна.

## 5. Аюулгүй байдлын талаар анхаарах зүйлс

Энэ үйлчилгээг үр дүнтэй болгохын тулд системийг ашигладаг гэрчилгээ нь гэрчилгээний төлөв байдлын үйлчилгээ үзүүлэгчтэй холбогдох ёстой. Ийм холболтыг олж авах боломжгүй тохиолдолд гэрчилгээ ашигладаг системүүд ХГЖ боловсруулах логикийг буцаах байрлал болгон хэрэгжүүлэх боломжтой.

Үйлчилгээг тасалдуулах эмзэг байдал нь маш их асуулга ирсэн тохиолдолд илт харагддаг. Криптограф гарын үсэг боловсруулах нь хариулт үүсгэх мөчлөгийн хугацаанд ихээхэн нөлөөлж, улмаар нөхцөл байдлыг улам хүндрүүлнэ. Гарын үсэг зураагүй алдааны хариу үйлдэл нь протоколыг өөр нэг үйлчилгээг эсэргүүцэх халдлагад нээж өгдөг бөгөөд халдагч нь  хуурамч алдаа илгээдэг.

Урьдчилан тооцоолсон хариултуудыг ашиглах нь хуучин (сайн) хариултыг хүчинтэй хугацаа нь дуусахаас өмнө, гэхдээ гэрчилгээг хүчингүй болгосны дараа дахин эхлүүлэх халдлагуудыг хийх боломжийг олгодог. ОГТБП -ийг байршуулахдаа давтан довтолгооны магадлал болон түүнийг амжилттай хэрэгжүүлэхтэй холбоотой зардлын эсрэг урьдчилан тооцоолсон хариултын ашиг тусыг сайтар үнэлэх хэрэгтэй.

Хүсэлт нь тэдний илгээсэн хариулагчийг агуулаагүй болно. Энэ нь халдагчид хүссэн тооны  ОГТБП хариулагчийн хүсэлтийг дахин давтах боломжийг олгодог.

Хэрэв завсрын серверүүд буруу тохируулагдсан эсвэл кэшийн удирдлагын алдаатай байгаа нь мэдэгдэж байгаа бол зарим байршуулалтын хувилбарт HTTP кэшийн найдвартай байдал нь гэнэтийн үр дүнд хүргэж болзошгүй юм. ОГТБП -ийг HTTP дээр байрлуулахдаа HTTP кэш механизмын найдвартай байдлыг харгалзан үзэхийг хэрэгжүүлэгч нарт зөвлөж байна.

## 6. Ашигласан материал


| | |
|---|---|
| [RFC2459] | Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999. |
| [HTTP] | Fielding, R., Gettys, J., Mogul, J., Frystyk, H. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997. |
| [RFC2119] | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. |
| [URL] | Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994. |
| [X.690] | ITU-T Recommendation X.690 (1994) \| ISO/IEC 8825-1:1995, Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). |


## 7. Зохиогчийн хаяг


**Michael Myers**

VeriSign, Inc. 1350 Charleston Road Mountain View, CA 94043

EMail: mmyers@verisign.com

**Rich Ankney**

CertCo, LLC 13506 King Charles Dr. Chantilly, VA 20151

EMail: rankney@erols.com

**Ambarish Malpani**

ValiCert, Inc. 1215 Terra Bella Ave. Mountain View, CA 94043 Phone: 650.567.5457

EMail: ambarish@valicert.com

**Slava Galperin**

My CFO, Inc. 1945 Charleston Road Mountain View, CA

EMail: galperin@mycfo.com

**Carlisle Adams**

Entrust Technologies 750 Heron Road, Suite E08 Ottawa, Ontario K1V 1A7 Canada

EMail: cadams@entrust.com

**Хавсралт А.**

**А.1 HTTP дэх ОГТБП**

Энэ хэсэгт HTTP-г дэмжих хүсэлт болон хариултад хийгдэх форматыг тайлбарлана.

**А.1.1 Хүсэлт**

HTTP-д суурилсан ОГТБП хүсэлтүүд нь GET эсвэл POST аргыг ашиглан хүсэлтээ илгээж болно. HTTP кэшийг идэвхжүүлэхийн тулд жижиг хүсэлтүүдийг (кодчилсны дараа 255 байтаас бага) GET ашиглан илгээж болно. Хэрэв HTTP кэш чухал биш эсвэл хүсэлт нь 255 байтаас их бол хүсэлтийг POST ашиглан илгээх ХЭРЭГТЭЙ. Нууцлалыг хангах шаардлагатай тохиолдолд HTTP ашиглан солилцсон ОГТБП гүйлгээг TLS/SSL эсвэл өөр доод түвшний протокол ашиглан хамгаалж болно.

GET аргыг ашиглан ОГТБП хүсэлтийг дараах байдлаар бүтээнэ:

> GET {url}/{url-encoding of base-64 encoding of the DER encoding of the OCSPRequest}

Энд {url} нь AuthorityInfoAccess-ийн утга эсвэл ОГТБП клиентийн бусад локал тохиргооноос үүсэлтэй байж болно.

POST аргыг ашиглан ОГТБП хүсэлтийг дараах байдлаар бүтээнэ: Content-Type гэсэн толгой хэсэг нь "application/ocsp-request" утгатай байхад мессежний үндсэн хэсэг нь OCSPRequest-ийн DER кодчиллын бинар буюу хоёртын утга юм.

**А.1.2 Хариулт**

HTTP-д суурилсан ОГТБП хариулт нь OCSPResponse-ийн DER кодчиллын хоёртын утгын дараа түүнд тохирсон HTTP толгой хэсгээс бүрдэнэ. Content-Type гэсэн толгой хэсэг нь "application/ocsp-response" гэсэн утгатай байна. Content-Length толгой хэсэгт хариултын уртыг зааж өгөх ёстой. Өөр HTTP толгойнууд байж болох ба хэрэв хүсэлт гаргагч ойлгохгүй байгаа бол түүнийг хэрэгсэхгүй орхиж болно.

**Хавсралт В. ХСТ.1 дэх ОГТБП**

```
OCSP DEFINITIONS EXPLICIT TAGS::=
BEGIN
IMPORTS
        -- Directory Authentication Framework (X.509)
                Certificate, AlgorithmIdentifier, CRLReason
                 FROM AuthenticationFramework { joint-iso-itu-t ds(5)
                        module(1) authenticationFramework(7) 3 }

-- PKIX Certificate Extensions
              AuthorityInfoAccessSyntax
          FROM PKIX1Implicit88 {iso(1) identified-organization(3)
                    dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                    id-mod(0) id-pkix1-implicit-88(2)}
         Name, GeneralName, CertificateSerialNumber, Extensions,
            id-kp, id-ad-ocsp
               FROM PKIX1Explicit88 {iso(1) identified-organization(3)
                      dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                      id-mod(0) id-pkix1-explicit-88(1)};

OCSPRequest         ::=         SEQUENCE {
       tbsRequest                          TBSRequest,
```

```
        optionalSignature      [0] EXPLICIT Signature OPTIONAL }

TBSRequest      ::=             SEQUENCE {
        version                 [0] EXPLICIT Version DEFAULT v1,
        requestorName       [1] EXPLICIT GeneralName OPTIONAL,
        requestList                 SEQUENCE OF Request,
        requestExtensions   [2] EXPLICIT Extensions OPTIONAL }

Signature    ::=                SEQUENCE {
        signatureAlgorithm  AlgorithmIdentifier,
        signature               BIT STRING,
        certs                   [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }

Version      ::=      INTEGER  { v1(0) }

Request  ::=          SEQUENCE {
        reqCert                         CertID,
        singleRequestExtensions         [0] EXPLICIT Extensions OPTIONAL }

CertID   ::=    SEQUENCE {
        hashAlgorithm               AlgorithmIdentifier,
        issuerNameHash      OCTET STRING, -- Hash of Issuer's DN
        issuerKeyHash       OCTET STRING, -- Hash of Issuers public key
        serialNumber        CertificateSerialNumber }

OCSPResponse  ::=     SEQUENCE {
        responseStatus          OCSPResponseStatus,
        responseBytes           [0] EXPLICIT ResponseBytes OPTIONAL }

OCSPResponseStatus   ::=  ENUMERATED {
        successful              (0),      --Response has valid confirmations
        malformedRequest        (1),      --Illegal confirmation request
        internalError           (2),      --Internal error in issuer
        tryLater                (3),       --Try again later
                                           --(4) is not used
        sigRequired             (5), --Must sign the request
        unauthorized            (6) --Request unauthorized
}

ResponseBytes      ::=          SEQUENCE {
        responseType        OBJECT IDENTIFIER,
        response            OCTET STRING }
BasicOCSPResponse           ::= SEQUENCE {
        tbsResponseData     ResponseData,
        signatureAlgorithm  AlgorithmIdentifier,
        signature           BIT STRING,
        certs               [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }

ResponseData            ::= SEQUENCE {
        version                     [0] EXPLICIT Version DEFAULT v1,
        responderID                 ResponderID,
        producedAt                  GeneralizedTime,
        responses                   SEQUENCE OF SingleResponse,
        responseExtensions [1]      EXPLICIT Extensions OPTIONAL }

ResponderID      ::=    CHOICE {
        byName   [1]    Name,
```

```
        byKey       [2]    KeyHash }

KeyHash     ::=     OCTET STRING   --SHA-1 hash of responder's public key
                                   --(excluding the tag and length fields)

SingleResponse    ::=     SEQUENCE {
        certID                          CertID,
        certStatus                      CertStatus,
        thisUpdate                      GeneralizedTime,
        nextUpdate              [0]     EXPLICIT GeneralizedTime OPTIONAL,
        singleExtensions        [1]     EXPLICIT Extensions OPTIONAL }

CertStatus    ::=     CHOICE {
        good                    [0]     IMPLICIT NULL,
        revoked                 [1]     IMPLICIT RevokedInfo,
        unknown                 [2]     IMPLICIT UnknownInfo }

RevokedInfo    ::=    SEQUENCE  {
        revocationTime                  GeneralizedTime,
        revocationReason        [0]     EXPLICIT CRLReason OPTIONAL }

UnknownInfo  ::=     NULL -- this can be replaced with an enumeration

ArchiveCutoff   ::=          GeneralizedTime

AcceptableResponses    ::=     SEQUENCE OF OBJECT IDENTIFIER

ServiceLocator     ::=     SEQUENCE {
        issuer      Name,
        locator     AuthorityInfoAccessSyntax }

-- Object Identifiers
id-kp-OCSPSigning               OBJECT IDENTIFIER ::= { id-kp 9 }
id-pkix-ocsp                    OBJECT IDENTIFIER ::= { id-ad-ocsp }
id-pkix-ocsp-basic              OBJECT IDENTIFIER ::= { id-pkix-ocsp 1 }
id-pkix-ocsp-nonce              OBJECT IDENTIFIER ::= { id-pkix-ocsp 2 }
id-pkix-ocsp-crl                OBJECT IDENTIFIER ::= { id-pkix-ocsp 3 }
id-pkix-ocsp-response           OBJECT IDENTIFIER ::= { id-pkix-ocsp 4 }
id-pkix-ocsp-nocheck            OBJECT IDENTIFIER ::= { id-pkix-ocsp 5 }
id-pkix-ocsp-archive-cutoff     OBJECT IDENTIFIER ::= { id-pkix-ocsp 6 }
id-pkix-ocsp-service-locator    OBJECT IDENTIFIER ::= { id-pkix-ocsp 7 }
END
```

**Хавсралт С. MIME бүртгэл**

**С.1 программ/ocsp-хүсэлт**

Хэнд: ietf-types@iana.org

Сэдэв: MIME медиа төрлийн программ/ОГТБП хүсэлтийг бүртгэх

MIME медиа төрлийн нэр: программ

MIME дэд төрлийн нэр: ОГТБП -хүсэлт

Шаардлагатай параметрүүд: Байхгүй

Нэмэлт параметрүүд: Байхгүй

Кодчилоход анхаарах зүйлс: хоёртын

Аюулгүй байдлын асуудал: Мэдээллийн хүсэлтийг явуулдаг. Энэ хүсэлт нь сонголтоор криптографийн гарын үсэгтэй байж болно.

Хамтын ажиллагаатай холбоотой анхаарах зүйлс: Байхгүй

Нийтлэгдсэн тодорхойлолт: Онлайн гэрчилгээний статусын протоколын IETF PKIX Ажлын хэсгийн төсөл - ОГТБП

Энэ төрлийн медиаг ашигладаг программууд: ОГТБП үйлчлүүлэгчид

Нэмэлт мэдээлэл:

Шидэт тоо(ууд): Байхгүй
Файлын өргөтгөл(үүд): .ORQ
Macintosh файлын төрлийн код(ууд): байхгүй

Нэмэлт мэдээлэл авахыг хүсвэл холбогдох хүн, и-мэйл хаяг:

Амбариш Малпани <ambarish@valicert.com>

Зориулалтын хэрэглээ: НИЙТЛЭГ

Зохиогч/Хянагчийг өөрчлөх:
Амбариш Малпани <ambarish@valicert.com>

**С.2 программ/ОГТБП -хариу**

Хэнд: ietf-types@iana.org

Гарчиг: MIME медиа төрлийн программын бүртгэл/ocsp-хариу MIME медиа төрлийн нэр: программ

MIME дэд төрлийн нэр: ocsp-response

Шаардлагатай параметрүүд: Байхгүй

Нэмэлт параметрүүд: Байхгүй

Кодчилоход анхаарах зүйлс: хоёртын

Аюулгүй байдлын талаар анхаарах зүйлс: Криптографаар гарын үсэг зурсан хариу илгээдэг

Хамтын ажиллагаатай холбоотой анхаарах зүйлс: Байхгүй

Нийтлэгдсэн тодорхойлолт: Онлайн гэрчилгээний статусын протоколын IETF PKIX Ажлын хэсгийн төсөл - ОГТБП

Энэ төрлийн медиа ашигладаг программууд: ОГТБП серверүүд

Нэмэлт мэдээлэл:

Шидэт тоо(ууд): Байхгүй

Файлын өргөтгөл(үүд): .ORS

Macintosh файлын төрлийн код(ууд): байхгүй

Нэмэлт мэдээлэл авахыг хүсвэл холбогдох хүн, и-мэйл хаяг:

Амбариш Малпани <ambarish@valicert.com>

Зориулалтын хэрэглээ: НИЙТЛЭГ

Зохиогч/Хянагчийг өөрчлөх:

Амбариш Малпани ambarish@valicert.com

**Зохиогчийн эрхийн бүрэн мэдэгдэл**



**Талархал**

RFC Editor функцийн санхүүжилтийг одоогоор Интернэтийн нийгэмлэгээс гаргасанд талархаж байна.