МОНГОЛ УЛСЫН СТАНДАРТ

Ангилалтын код 3161

Интернэт X.509 Нийтийн Түлхүүрийн Дэд бүтэц - Цагийн бүртгэлийн (тамгалах) протокол (ЦБП)	**MNS xxxx**
Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	**RFC 3161**

Хураангуй

Энэ баримт бичигт Цагийн бүрд гэлийн үйлчилгээ үзүүлэгч-д (цаашид ЦБҮҮ гэх) илгээж буй хүсэлт болон ирж буй хариуны форматыг тодорхойлсон. Түүнчлэн ЦБҮҮ-ийн хүсэлтийг боловсруулахаас эхлээд хариу үүсгэх хүртэл үйл ажиллагаанд тавигдах аюулгүй байдлын хэд хэдэн шаардлагыг тогтоосон.

1. Танилцуулга

Цаг бүрд гэлийн үйлчилгээ нь тухайн өгөгдөл тодорхой цаг хугацаанаас өмнө байсан гэдгийг батлах нотолгоог дэмждэг. Хэдийгээр үйл ажиллагааны бусад загвар байж болох ч (жишээлбэл байгууллагын дотоодод цагийн бүрд гэл (тамгалах) хийхийн тулд ЦБҮҮ шаардагдаж болно) ЦБҮҮ нь итгэмжлэгдсэн гуравдагч талын (ИГТ) үйлчилгээ хэлбэрээр ажиллах нь зохистой.

Үл татгалзах шинжийг хангах үйлчилгээ (ҮТШХҮ) нь заасан хугацаанаас өмнө тухайн өгөгдөл байсан гэдгийг тогтоох боломжийг шаарддаг. Энэ протоколыг иймэрхүү үйлчилгээг дэмжих суурь болгон ашиглаж болно. Нийтийн түлхүүрийн гэрчилгээний хүчинтэй байх хугацаанд тоон гарын үсгийг бий болгосон гэдгийг хэрхэн нотлох жишээг хавсралтад үзүүлсэн.

Энэ баримт бичигт ашигласан "ЗААВАЛ", "БОЛОХГҮЙ", "ШААРДЛАГАТАЙ", "ХЭРЭГТЭЙ", "ХЭРЭГГҮЙ", “ЁСТОЙ", "ЗӨВЛӨСӨН", "БАЙЖ БОЛНО", "ЗААВАЛ БИШ" гэсэн түлхүүр үгс (том үсгээр, харуулсан)-ийг [RFC2119]-д тодорхойлсны дагуу тайлбарлана.

Өгөгдлийг цаг хугацааны тодорхой цэгтэй холбохын тулд Цагийн бүрд гэлийн үйлчилгээ үзүүлэгч (ЦБҮҮ) ашиглах шаардлагатай байж болно. Энэхүү Итгэмжлэгдсэн гуравдагч этгээд нь тухайн өгөгдлийн хувьд "оршин байсан тухай нотлох баримт"-ыг агшин зуур гаргаж өгдөг.

ЦБҮҮ-ийн үүрэг роль нь өгөгдөл тодорхой цаг хугацааны өмнө байсан гэдэг нотолгоог бий болгохын тулд өгөгдөлд цагийн бүрд гэлийн тэмдэглэгээ (тамга) тавихад оршино. Үүнийг жишээ нь, холбогдох гэрчилгээг хүчингүй болгохоос өмнө мэдээлэлд тоон гарын үсэг зурсан гэдгийг шалгахад цагийн бүрд гэлийг ашиглаж болох бөгөөд үүний үр дүнд гэрчилгээг хүчингүй болгохоос өмнө зурсан тоон гарын үсгийг шалгахад хүчингүй болсон нийтийн түлхүүрийн гэрчилгээг ашиглах боломжтой болно. Энэ нь нийтийн түлхүүрийн дэд бүтцийн чухал үйл ажиллагааны нэг юм. ЦБҮҮ-ийн

үйлчилгээг илгээсэн хугацааг (эцсийн хугацаа чухал бол) зааж өгөх юм уу бүрд гэлийн журналд оруулахын тулд гүйлгээний цагийг зааж өгөхөд ашиглаж болно. ЦБҮҮ-ийн үйлчилгээний боломжит хэрэглээний бүрэн жагсаалт энэ баримт бичгийн хамрах хүрээнд орохгүй.

Энэ стандарт нь бусад PKIX стандартууд ГОБ-ын үйл ажиллагаанд тавигдах шаардлагыг тогтоодоггүйтэй нэгэн адил ЦБҮҮ-ийн үйл ажиллагаанд тавигдах аюулгүй байдлын ерөнхий шаардлагуудыг тогтоохгүй. Харин цагийн бүрд гэлийг зөв үүсгэх үйл явцыг хангахын тулд хэрэгжүүлж буй бодлогоо боломжит үйлчлүүлэгчид мэдэгдэх, эдгээр бодлого нь үйлчлүүлэгчдийн хэрэгцээ шаардлагад нийцэж байгаа гэдэгт тэд итгэлтэй байгаа тохиолдолд ЦБҮҮ-ийн үйлчилгээг ашиглах явцад үйлчлэх боломжтой.

2. ЦБҮҮ

ЦБҮҮ гэж өгөгдөл тодорхой цаг хугацаанд оршин байсан гэдгийг нотлох, илэрхийлэхийн тулд цагийн бүрд гэлийн токен үүсгэж буй ИГТ-ыг хэлнэ.

Баримт бичгийн дараах хэсгүүдэд “хүчин төгөлдөр хүсэлт” гэж зөв тайлагдаж уншигддаг, 2.4-т заасан хэлбэртэй, ЦБҮҮ-ийн захиалагчаас (үйлчлүүлэгч) ирсэн хүсэлтийг ойлгоно.

2.1. ЦБҮҮ-д тавигдах шаардлага

ЦБҮҮ дараах шаардлагыг хангах ёстой:

1. цагийн итгэлтэй эх сурвалж ашиглах.
2. цагийн бүрд гэлийн токен (цаашид “токен” гэх) бүрд цагийн итгэлтэй утгыг оруулах.
3. шинээр үүсгэж буй токен бүрд хосгүй бүхэл тоо оруулах.
4. боломжтой бол хүсэлт гаргагчаас хүчин төгөлдөр хүсэлт хүлээн авсны дараа токен үүсгэх.
5. токенийг олгоход баримталсан аюулгүй байдлын бодлогыг хөдөлбөргүй зааж өгөхийн тулд олгож буй токен бүрд адилтгагч (нэр) оруулж өгөх.
6. Өгөгдлийн хэш илэрхийлэлд цагийн бүрд гэл (тамга тавих) хийх, ө.х OID-ын тусламжтайгаар хөдөлбөргүй адилтгагддаг, нэг чиглэлийн зөрчилдөөнд тэсвэртэй хэш функцтэй холбоотой өгөгдлийн дардас тавих
7. Нэг талын, зөрчилдөөнт тэсвэртэй хэш функцийн OID-ийг шалгах болон хэш утгын урт нь хэшлэх алгоритмтай нийцэж байгааг баталгаажуулах.
8. Цагийн бүрд гэл хийгдсэн (тамга дарагдсан) дардсыг ямар нэг аргаар шалгахгүй байх (өмнөх хэсэгт зааснаар уртыг нь хэмжихээс өөрөөр).
9. Цагийн бүрд гэлийн токенд хүсэлт гаргагчийг адилтгах аливаа мэдээлэл оруулахгүй байх.
10. Цагийн бүрд гэл бүхий токенд зөвхөн энэ зорилгоор үүсгэсэн түлхүүрээр гарын үсэг зурах, түлхүүрийн энэ онцлогийг зохих гэрчилгээнд зааж өгөх.

11. ЦБҮҮ-ийн дэмжиж буй өргөтгөлийн хувьд хүсэлт гаргагч өргөтгөлийн талбарыг ашиглан хүсэлт гаргасан бол цагийн бүрд гэлийн токенд нэмэлт мэдээлэл оруулах. Хэрэв энэ боломжгүй бол ЦБҮҮ-ээс алдааны тухай мэдээлэл хариу илгээх ёстой.

2.2. ЦБҮҮ-ийн транзакци (мэдэгдэл солилцоо)

Хүсэлт гаргагч этгээд ЦБҮҮ-ийн системийн эхний мэдэгдэл (мессеж) байдлаар ЦБҮҮ-д цагийн бүрд гэлийн токен хүссэн хүсэлтийг (доор тодорхойлсон TimeStampReq, эсхүл түүнийг агуулсан) илгээнэ. Хоёр дахь мэдэгдэл байдлаар ЦБҮҮ-ээс хүсэлт гаргагчид хариу (доор тодорхойлсон TimeStampResp, эсхүл түүнийг агуулсан) илгээнэ.

Хүсэлт гаргагч этгээд хариу (доор тодорхойлсноор цагийн бүрд гэлийн токен - TimeStampToken (ЦБТ) агуулсан TimeStampResp юм уу түүнийг агуулсан) хүлээн авсны дараа хариу дахь төлөвийн алдааг шалгах ЁСТОЙ, хэрэв алдаа байхгүй бол TimeStampToken - ЦБТ -д байх янз бүрийн талбарууд болон TimeStampToken - ЦБТ дахь тоон гарын үсгийн хүчин төгөлдөр байдлыг шалган баталгаажуулах ЁСТОЙ. Тухайлбал цагийн бүрд гэл хийгдсэн зүйл нь цагийн бүрд гэл хийлгэхээр хүссэн зүйлтэй нийцэж байгааг баталгаажуулах ЁСТОЙ. Хүсэлт гаргагч нь ЦБТ-д ЦБҮҮ-ийн гэрчилгээний зөв нэр, адилтгагч, өгөгдлийн зөв дардас, хэш алгоритмын зөв OID оруулсан гэдгийг баталгаажуулах ЁСТОЙ. Дараа нь хариунд агуулагдаж буй цагийг итгэлтэй эталон цагтай (хэрэв байгаа бол) тулган шалгах юм уу хариунд агуулагдсан нэг удаагийн дугаарын (client программ зөвхөн нэг удаа үүсгэсэн байх магадлалтай тохиолдлын том тоо) утгыг хүсэлтэд агуулагдсан утгатай харьцуулах замаар цаг хугацаандаа хариу ирсэн эсэхийг шалгах ЁСТОЙ.

Хариултгай холбоотой халдлагыг илрүүлэх талаар илүү мэдээллийг аюулгүй байдлын асуудал хэсгээс (6-р зүйл) үзнэ үү. Дээр дурдсан баталгаажуулалтын аль нэг нь бүтэлгүй болбол TimeStampToken-ЦБТ -оос татгалзах ЁСТОЙ.

ЦБҮҮ-ийн гэрчилгээний хугацаа дуусах учир дараа нь гэрчилгээ хүчинтэй байгаа гэдэгт итгэлтэй байхын тулд гэрчилгээний төлөвийг шалгах (жишээ нь зохих хүчингүй гэрчилгээний жагсаалтыг (ХГЖ) шалгах замаар) ШААРДЛАГАТАЙ.

Дараа нь клиент программ нь токенийг ашиглахад баримтлах бодлоготой нийцэж, тохирч байгаа эсэхийг тодорхойлохын тулд бодлогын талбарыг шалгах ЁСТОЙ.

2.3. ЦБҮҮ-ийг адилтгах

ЦБҮҮ цагийн бүрд гэлийн мэдэгдэл бүрд зөвхөн тухайн зорилгод зориулсан түлхүүрээр гарын үсэг зурах ЁСТОЙ. ЦБҮҮ өөр өөр бодлого, өөр өөр алгоритм, өөр өөр хэмжээтэй хувийн түлхүүртэй байхын тулд, эсхүл гүйцэтгэлээ дээшлүүлэхийн тулд янз бүрийн хувийн түлхүүртэй байж БОЛНО. Хамаарах гэрчилгээ нь [RFC2459]-ын 4.2.1.13-д тодорхойлсон, KeyPurposeID утгатай түлхүүрийн ашиглалтын өргөтгөсөн талбарын зөвхөн нэг жишээг агуулах ЁСТОЙ:

id-kp-timeStamping Энэ өргөтгөл онц чухалд тооцогдож байх ЁСТОЙ.

Доор үзүүлсэн объектын адилтгагч нь id-kp-timeStamping утгатай KeyPurposeID-г адилтгаж тодорхойлно.

```
id-kp-timeStamping OBJECT IDENTIFIER ::= {iso(1)
        identified-organization(3) dod(6)
        internet(1) security(5) mechanisms(5) pkix(7)
        kp (3) timestamping (8)}
```

2.4. Хүсэлт болон Хариуны формат

2.4.1. Хүсэлтийн Format

Цагийн бүрд гэлийн хүсэлт дараах хэлбэртэй байна:

```
TimeStampReq ::= SEQUENCE {
   version INTEGER { v1(1) },
   messageImprint MessageImprint,
       --a hash algorithm OID and the hash value of the data to be
       --time-stamped
reqPolicy TSAPolicyId OPTIONAL,
nonce INTEGER OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
extensions [0] IMPLICIT Extensions OPTIONAL }
```

Хувилбарын талбар (одоо v1) Цагийн бүрд гэлийн хүсэлтийн хувилбарыг тодорхойлно.

MessageImprint - талбар нь цагийн бүрд гэл тавих ёстой өгөгдлийн хэшийг агуулах ЁСТОЙ. Хэш нь OCTET STRING хэлбэрээр илэрхийлэгдэнэ. Түүний урт нь тухайн алгоритмын хэш утгын урттай ЗААВАЛ таарч байх ёстой. (жишээ нь, SHA-1-ийн хувьд 20 байт эсхүл MD5-ын хувьд 16 байт).

MessageImprint ::= SEQUENCE {

hashAlgorithm AlgorithmIdentifier,

hashedMessage OCTET STRING }

hashAlgorithm талбарт заасан хэш алгоритм нь илт мэдэгддэг хэшлэлийн алгоритм (нэг чиглэлтэй, зөрчилдөөнд тэсвэртэй) байх ЁСТОЙ. Энэ нь нэг чиглэлтэй, зөрчилдөөнд тэсвэртэй байх ЁСТОЙ гэсэн үг. ЦБҮҮ тухайн хэш алгоритм нь "хангалттай" (жишээ нь крипто шинжилгээний өнөөгийн мэдлэг болон тооцооллын нөөцийн хөгжлийн орчин үеийн түвшинд үндэслэн) гэдгийг шалгах ЁСТОЙ. Хэрэв ЦБҮҮ хэш алгоритмыг мэдэхгүй эсхүл хэш алгоритм нь сул байгааг мэдэж байвал (шийдвэрийг ЦБҮҮ тус бүр өөрийн үзэмжээр гаргана) "bad_alg" гэсэн утгатай pkiStatusInfo-г буцаан илгээж, цагийн бүрд гэлийн токен олгохоос татгалзах ЁСТОЙ.

Хэрэв reqPolicy талбар орсон бол TimeStampToken-г олгоход баримтлах ёстой ЦБҮҮ-ийн бодлогыг заасан байна. TSAPolicyId талбар дараах байдлаар тодорхойлогддог:

TSAPolicyId ::= OBJECT IDENTIFIER

Хэрэв нэг удаагийн тохиолдлын тоо - nonce оруулсан бол түүний утга нь орон нутгийн цагт хандах боломжгүй үед хариу цаг хугацаандаа ирсэн гэдгийг шалгах боломжийг үйлчлүүлэгчид олгодог. Nonce гэдэг нь client програм зөвхөн нэг удаа үүсгэсэн байх магадлалтай тохиолдлын том тоо (жишээ нь, 64 битийн бүхэл тоо). Энэ тохиолдолд ижил утгатай nonce -ийг хариунд оруулах ЁСТОЙ, эс тэгвээс хариунаас татгалзана.

Хэрэв certReq талбар байгаа бөгөөд үнэн гэсэн утгатай байвал хариу мэдэгдэл дахь SigningCertificate атрибут шинжийн доторх ESSCertID адилтгагчийн зааж өгч буй ЦБҮҮ-ийн нийтийн түлхүүрийн гэрчилгээг тухайн хариулт дахь SignedData structure -ийн гэрчилгээний талбараар дамжуулан ЦБҮҮ гаргаж өгөх ЁСТОЙ. Энэ талбар нь бусад гэрчилгээг агуулж болно.

Хэрэв certReq талбар байхгүй, эсхүл байгаа боловч false утгатай байвал SignedData structure-ийн гэрчилгээний талбарыг хариунд оруулахгүй байх ЁСТОЙ.

Өргөтгөлийн талбар нь хүсэлтэд нэмэлт мэдээлэл оруулах нийтлэг арга юм. Өргөтгөлүүдийг [RFC 2459]-д тодорхойлсон. Хэрэв хүсэлт гаргагчийн ашиглаж буй өргөтгөл чухал юм уу чухал биш гэж тэмдэглэгдсэн эсэхээс үл хамааран цагийн бүрд гэлийн серверт танигдаагүй бол сервер токен олгохгүй байх ЁСТОЙ бөгөөд татгалзсан хариу (unacceptedExtension) өгөх ЁСТОЙ.

Цагийн бүрд гэлийн хүсэлт нь хүсэлт гаргагчийг тодорхойлохгүй, учир нь энэ

мэдээллийг ЦБҮҮ шалгадаггүй (2.1-ийг үзнэ үү). ЦБҮҮ хүсэлт гаргагчийг адилтгах, таних шаардлагатай нөхцөлд адилтган таних / баталгаажуулах өөр хэрэгслийг ашиглах шаардлагатай (жишээ нь, CMS encapsulation [CMS] эсхүл TLS баталгаажуулалт [RFC2246]).

2.4.2. Хариуны (мэдэгдлийн) формат

Цагийн бүрд гэлийн хүсэлтийн хариу (мэдэгдэл) дараах хэлбэрээр харагдана:

```
TimeStampResp ::= SEQUENCE {
    status PKIStatusInfo,
    timeStampToken TimeStampToken OPTIONAL }
```

Төлөв-статус нь [RFC2510] -ын 3.2.3-т тусгасан төлөвийн тодорхойлолтод суурилах бөгөөд дараах хэсэгт тусгасан илэрхийлэлтэй байна:

```
PKIStatusInfo ::= SEQUENCE {
    status PKIStatus,
    statusString PKIFreeText OPTIONAL,
    failInfo PKIFailureInfo OPTIONAL }
```

Төлөв-статус нь “тэг” юм уу “нэг” гэсэн утгыг агуулж байвал TimeStampToken ЗААВАЛ байх ёстой. Төлөв нь “тэг” юм уу “нэг”-ээс өөр утгыг агуулж байвал TimeStampToken БАЙЖ болохгүй. Төлөв хэсэгт дараах утгуудын аль нэг агуулагдаж байх ёстой:

```
PKIStatus ::= INTEGER {
    granted (0),
    -- when the PKIStatus contains the value zero a TimeStampToken, as
    requested, is present.
    grantedWithMods (1),
    -- when the PKIStatus contains the value one a TimeStampToken,
    with modifications, is present.
    rejection (2),
    waiting (3),
    revocationWarning (4),
    -- this message contains a warning that a revocation is
    -- imminent
    revocationNotification (5)
    -- notification that a revocation has occurred }
```

Нийцэлтэй серверүүд өөр ямар нэг утгыг үүсгэж (гаргаж) болохгүй. Нийцэлтэй клиент программууд ойлгогдохгүй утга байгаа тохиолдолд алдаа заах ЁСТОЙ. TimeStampToken байхгүй байгаа үед failInfo нь цагийн бүрд гэлийн хүсэлтээс татгалзсан шалтгааныг заадаг бөгөөд дараах утгуудын аль нэгийг авсан байж болно.

```
PKIFailureInfo ::= BIT STRING {
    badAlg (0),
    -- unrecognized or unsupported Algorithm Identifier
```

badRequest (2),
-- transaction not permitted or supported
badDataFormat (5),
-- the data submitted has the wrong format
timeNotAvailable (14),
-- the TSA’s time source is not available
unacceptedPolicy (15),
-- the requested TSA policy is not supported by the TSA
unacceptedExtension (16),
-- the requested extension is not supported by the TSA
addInfoNotAvailable (17)
-- the additional information requested could not be understood
-- or is not available systemFailure (25)
-- the request cannot be handled due to system failure }

Эдгээр нь зөвхөн PKIFailureInfo-ийн дэмжих ЁСТОЙ утгууд юм.

Нийцэлтэй серверүүд өөр ямар ч утгыг үүсгэж БОЛОХГҮЙ. Нийцэлтэй клиент программууд ойлгохгүй утга байгаа тохиолдолд алдаа заах ЁСТОЙ.

PKIStatusInfo дахь statusString талбарыг "messageImprint field is not correctly formatted" гэх мэт шалтгааныг заасан бичвэр оруулахад ашиглаж БОЛНО.

TimeStampToken нь дараах байдлаар харагдана. Энэ нь ContentInfo ([CMS]) гэж тодорхойлогдох бөгөөд гарын үсэг зурсан өгөгдлийн агуулгын төрлийг багтаасан байх ёстой.

TimeStampToken ::= ContentInfo
-- contentType is id-signedData ([CMS])
-- content is SignedData ([CMS])

SignedData бүтцийн EncapsulatedContentInfo төрлийн талбар дараах утгатай байна:

eContentType нь агуулгын төрлийг хөдөлбөргүй тодорхойлдог объектын адилтгагч байна. ЦБТ-ий хувьд энэ нь дараах байдлаар тодорхойлогдоно:

id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

eContent гэдэг нь октетт мөр байдлаар илэрхийлэгдэж буй агуулга өөрөө байна. eContent нь DER шифрлэгдсэн (кодлогдсон) TSInfo-ийн утга байх ёстой.

Цагийн бүрд гэлийн токен (ЦБТ) нь ЦБҮҮ-ийн гарын үсгээс өөр гарын үсэг агуулж БОЛОХГҮЙ. ЦБҮҮ-ийн гэрчилгээний адилтгагч (ESSCertID) нь SigningCertificate атрибут шинж дотор signerInfo атрибут шинж байдлаар орсон байх ЁСТОЙ.

TSTInfo ::= SEQUENCE {
version INTEGER { v1(1) },
policy TSAPolicyId,
messageImprint MessageImprint,

-- MUST have the same value as the similar field in
-- TimeStampReq
serialNumber INTEGER,
-- Time-Stamping users MUST be ready to accommodate integers
-- up to 160 bits.
genTime GeneralizedTime,
accuracy Accuracy OPTIONAL,
ordering BOOLEAN DEFAULT FALSE,
nonce INTEGER OPTIONAL,
-- MUST be present if the similar field was present
-- in TimeStampReq. In that case it MUST have the same value.
tsa [0] GeneralName OPTIONAL,
extensions [1] IMPLICIT Extensions OPTIONAL }

Хувилбарын талбар (одоо v1) нь цагийн бүрд гэлийн токений хувилбарыг тодорхойлдог.

Цагийн бүрд гэлийн нийцэлтэй серверүүд ЗААВАЛ 1-р хувилбарын токен олгох боломжтой байх ёстой.

Нэмэлт талбаруудаас зөвхөн nonce талбарыг дэмжих ЁСТОЙ. Цагийн бүрд гэлийн хүсэлт гаргагч (нийцэлтэй) 1-р хувилбарын цагийн бүрд гэлийн токеныг бүх нэмэлт талбартай нь хамт таних боломжтой байх ЁСТОЙ, гэхдээ хэрэв байгаа бол аливаа өргөтгөлийн семантикийг ойлгох албагүй.

Бодлогын талбар нь хариуг бэлтгэхдээ баримталсан ЦБҮҮ-ийн бодлогыг ЗААВАЛ зааж өгөх ёстой. Хэрэв TimeStampReq-д ижил төстэй талбар байгаа бол энэ нь ижил утгатай байх ёстой, тийм биш бол алдаа (unacceptedPolicy) зааж буцаах ЁСТОЙ.

Энэхүү бодлого нь дараах төрлийн мэдээллийг агуулж БОЛНО (гэхдээ энэ жагсаалт бүрэн дүүрэн биш):

* ЦБТ-ийг ашиглаж болох нөхцөл.
* ЦБТ үнэн зөв гэдгийг сүүлд нь баталгаажуулахын тулд ЦБТ-ны лог бүрд гэлийн хүртээмжтэй байдал

Хэш утгын хэмжээ нь hashAlgorithm-д тодорхойлсон хэш алгоритмын хүлээгдэж буй хэмжээтэй таарч байгаа тохиолдолд messageImprint нь TimeStampReq дээрх ижил төстэй талбартай ижил утгатай байх ЁСТОЙ.

serialNumber талбар нь ЦБҮҮ-ээс ЦБТ бүрд оноосон бүхэл тоо юм. Энэ тоо нь тухайн ЦБҮҮ-ээс олгож буй ЦБТ бүрд хосгүй (өөрөөр хэлбэл, ЦБҮҮ-ийн нэр болон серийн дугаар нь хосгүй, давхцахгүй ЦБТ-ийг тодорхойлдог) байх ЁСТОЙ. Эдгээр шинжүүд үйлчилгээний болзошгүй саатал, тасалдлын (жишээ нь, гэмтэх) дараа ч хадгалагдаж байх ЁСТОЙ гэдгийг анхаарах хэрэгтэй.

genTime гэж ЦБҮҮ-ээс ЦБТ-ийг үүсгэсэн цаг юм. Орон нутгийн цагийн бүсийн ашиглалттай хольж хутгах, төөрөгдөлд орохыг багасгахын тулд ДУЦ - UTC цагаар

(Дэлхийн уялдуулсан цаг) илэрхийлнэ. ДУЦ гэж CCIR[1]-аас тодорхойлж, санал болгосон, Олон улсын хэмжүүр, жингийн товчоогоор (BIPM) дэмжигддэг секунд (SI) дээр суурилсан цагийн хуваарь юм. Ижил төстэй цаг нь иргэний нисэхийн ашигладаг "Zulu" цаг бөгөөд "Z" үсгээр илэрхийлэгддэг (дуудлага нь "Зулу").

ASN.1 GeneralizedTime синтакс нь миллисекундын нарийвчлалтай мэдээллийг агуулж болно. GeneralizedTime нь цагийг нэг секундийн нарийвчлалтай илэрхийлэхээр хязгаарлагдсан байдаг тул [RFC 2459]-ын 4.1.2.5.2-д тусгаснаар ямар нэг хязгаарлалтгүй ийм синтаксийг энд ашиглаж болно.

GeneralizedTime-ын утга ЗААВАЛ секундийг агуулна. Гэхдээ секундээс илүү нарийвчлалтай байх шаардлагагүй бол нэг секундээр хязгаарлагдах нарийвчлалтай GeneralizedTime-ийг ашиглах ХЭРЭГТЭЙ ([RFC 2459]-д тусгасантай ижил).

The syntax is: YYYYMMDDhhmmss[.s...]Z
Example: 19990609001326.34352Z

X.690 | ISO/IEC 8825-1-д DER шифрлэлтэд тавигдах дараах хязгаарлалтыг тодорхойлсон.

Шифрлэлт нь “Z” үсгээр (“Zulu” цаг гэсэн утгатай) төгссөн байх ЁСТОЙ. Хэрэв аравтын цэгийн элемент байгаа бол "." гэсэн цэгийн сонголт байх ЁСТОЙ.

Хэрэв секундгүй долийн элементүүд байгаа бол төгсгөлийн бүх 0-ийг орхих ЁСТОЙ; Хэрэв элементүүд нь 0-тэй тохирч байвал тэдгээрийг бүхэлд нь орхих ЁСТОЙ ба аравтын бутархай элементийг мөн орхих ЁСТОЙ.

Шөнө дундыг (GMT) "YYYYMMDD000000Z" хэлбэрээр илэрхийлнэ. Энд "YYYYMMDD" нь тухайн шөнө дундын дараах өдрийг илэрхийлнэ.

Энд хүчинтэй илэрхийллийн зарим жишээг харуулав:

"19920521000000Z"
"19920622123421Z"
"19920722132100.3Z"

Нарийвчлал - accuracy нь GeneralizedTime-д агуулагдах ДУЦ дахь цагийн гажилтыг илэрхийлнэ.

```
Accuracy ::= SEQUENCE {
        seconds INTEGER OPTIONAL,
        millis [0] INTEGER (1..999) OPTIONAL,
        micros [1] INTEGER (1..999) OPTIONAL }
```

Хэрэв секунд, миллсекунд (доль) эсвэл микро секундийн аль нэг нь дутуу байвал дутуу талбарт 0 гэсэн утгыг ЗААВАЛ өгнө. Нарийвчлалын утгыг GeneralizedTime-д нэмснээр ЦБҮҮ-ээс ЦБТ үүсгэж байх үеийн хугацааны дээд хязгаарыг олж авах боломжтой. Үүний нэгэн адил нарийвчлалыг GeneralizedTime-аас хассанаар ЦБҮҮ-ээс ЦБТ үүсгэж байх үеийн хугацааны доод хязгаарыг олж авах боломжтой.

[1] Consultative Committee on Radio Communications

Нарийвчлалыг секунд, миллсекунд (1-999 хооронд) болон микросекундэд (1-999) задлах боломжтой бөгөөд бүгдийг бүхэл тоогоор илэрхийлнэ.

Нарийвчлалын нэмэлт талбар байхгүй байгаа тохиолдолд нарийвчлалыг TSAPolicyId гэх мэт өөр хэрэгслээр тодорхойлох боломжтой.

Хэрэв захиалгын талбар байхгүй эсвэл захиалгын талбар байгаа боловч false гэсэн утгатай бол genTime талбар нь зөвхөн ЦБҮҮ-ээс цагийн тэмдэг үүсгэсэн цагийг заана. Энэ тохиолдолд нэг ЦБҮҮ-ээс, эсхүл өөр өөр ЦБҮҮ-ээс олгох ЦБТ захиалах нь зөвхөн эхний ЦБТ-ны genTime болон хоёр дахь ЦБТ-ны genTime хоорондын зөрүү нь ЦБТ бүрийн genTime-ийн нарийвчлалын нийлбэрээс их байх үед л боломжтой.

Хэрэв захиалгын талбар байгаа бөгөөд true гэсэн утгатай бол genTime-ийн нарийвчлалаас үл хамааран нэг ЦБҮҮ-ийн олгосон ЦБТ бүрийг genTime талбарт үндэслэн захиалж болно.

Хэрэв TimeStampReq-д nonce талбар байгаа бол тухайн талбар ЗААВАЛ БАЙХ ЁСТОЙ. Энэ тохиолдолд тухайн талбар нь TimeStampReq бүтцэд заасан утгатай тэнцүү байх ёстой.

tsa талбарын зорилго нь ЦБҮҮ-ийн нэрийг зааж өгөхөд оршино. Хэрэв энэ талбар байгаа бол токенийг баталгаажуулахад ашиглагдах гэрчилгээнд орсон субъектүүдийн аль нэгнийх нь нэртэй таарч байх ЁСТОЙ. Гэхдээ, хариунд гарын үсэг зурсан этгээдийг бодитой адилтган таних ажиллагаа signerInfo-ийн нэг хэсэг болох SigningCertificate атрибут шинж доторх гэрчилгээний адилтган танигч (ESSCertID Аттрибут)-ыг ашиглах замаар хийгдэнэ ([ESS]-ийн 5-р хэсгийг үзнэ үү).

extensions - өргөтгөлүүд нь ирээдүйд нэмэлт мэдээлэл нэмэх нийтлэг арга юм. Өргөтгөлүүдийг [RFC 2459]-д тодорхойлсон.

Өргөтгөлийн тодорхой талбарын төрлийг стандартад зааж өгөх юм уу ямар нэг байгууллага, нийгэмлэг тодорхойлж, бүрд гэж болно.

3. Тээвэрлэлт (дамжуулалт)

ЦБҮҮ-ийн мэдэгдлийг тээвэрлэх, заавал байх механизмын талаар энэ баримт бичигт заагаагүй. Доор тодорхойлсон механизмуудаас сонгон хэрэглэж болно; нэмэлт боломжтой механизмыг ирээдүйд тодорхойлж болно.

3.1. И-мэйл ашигласан Цагийн бүрд гэлийн протокол

Энэ хэсэгт 2-р бүлэг болон Хавсралт D-д тусгасан, протокол солилцоход зориулсан ASN.1-ээр шифрлэгдсэн мэдэгдлийг (мессеж) интернэт шуудангаар дамжуулах хэрэгслийг тодорхойлсон.

MIME хоёр объектыг дараах байдлаар тодорхойлсон:

Content-Type: application/timestamp-query
Content-Transfer-Encoding: base64
<<the ASN.1 DER-encoded Time-Stamp message, base64-encoded>>

Content-Type: application/timestamp-reply

Content-Transfer-Encoding: base64
<<the ASN.1 DER-encoded Time-Stamp message, base64-encoded>>

Эдгээр MIME объектуудыг MIME боловсруулалтын энгийн механизмыг ашиглан илгээж, хүлээн авах боломжтой бөгөөд цагийн бүрд гэлийн мэдэгдлийг энгийн интернэт шуудангаар тээвэрлэх (дамжуулах) боломжийг хангадаг.

MIME төрлийн бүх аппликейшн программ / цагийн бүрд гэлийн хүсэлт болон аппликейшн программ / цагийн бүрд гэлийн хариуг хэрэгжүүлэхэд сонголтоор "name" болон "filename" параметр үзүүлэлтийг агуулж байх ЁСТОЙ. Файлын нэрийг оруулах нь цагийн тэмдгийн хүсэлт болон хариуг файл болгон хадгалах үед төрлийн талаарх мэдээллийг хадгалахад тусалдаг. Эдгээр параметр үзүүлэлтийг оруулсан тохиолдолд тохирох өргөтгөлтэй файлын нэрийг сонгох ЁСТОЙ:

MIME Type	File Extension
application/timestamp-query	.TSQ
application/timestamp-reply	.TSR

Түүнээс гадна файлын нэр нь найман тэмдэгтээр хязгаарлагдаж байх ЁСТОЙ бөгөөд араас нь гурван үсэгтэй өргөтгөл байна. Найман тэмдэгттэй файлын нэрийн суурь нь ямар ч нэр байж болно.

3.2. Файлд суурилсан протокол

Цагийн бүрд гэлийн мэдэгдэл агуулсан файл нь ЦБҮҮ-ийн зөвхөн нэг мэдэгдлийн DER шифрлэлт агуулсан байх ЁСТОЙ, өөрөөр хэлбэл файлд ямар ч гаднын гарчиг юм уу дагалт мэдээлэл байх ЁСГҮЙ. Жишээ нь FTP ашиглан цагийн бүрд гэлийн мэдэгдлийг тээвэрлэхэд ийм файлыг ашиглаж болно.

Цагийн бүрд гэлийн хүсэлт .tsq өргөтгөлтэй файлд (Time-Stamp Query-тэй нэгэн адил) агуулагдах ЁСТОЙ. Цагийн бүрд гэлийн хариу нь .tsr өргөтгөлтэй файлд (Time-Stamp Reply-тай нэгэн адил) агуулагдах ЁСТОЙ.

3.3. Сокет үүрэнд суурилсан протокол

TCP-д суурилсан дараах энгийн протоколыг ЦБҮҮ-ийн мэдэгдлийг (мессеж) тээвэрлэхэд ашиглах ёстой. Объект ажиллагааг эхлүүлж, үр дүнг хүсэж байгаа үед энэ протокол тохиромжтой.

ЦБҮҮ-ийн мэдэгдлийг нягт зөв тодорхойлсон порт (IP портын дугаар 318)-оор дамжуулан ЦБҮҮ-д хүлээн авах үед чагнах үйл явцыг энэхүү протокол илэрхийлдэг.

Ерөнхийдөө санаачлагч энэ порт руу холбогдож, ЦБҮҮ-ийн анхны мэдэгдлийг (мессеж) илгээдэг. Хариулагч ЦБҮҮ-ийн мэдэгдэл юм уу дараа нь TSA мэдэгдлийн бодит хариуг хүсэх үед ашиглагдаж болох эшлэл - лавлагааны дугаарыг хариу болгон илгээнэ.

Хэрэв тухай хүсэлтэд ЦБҮҮ-ийн хэд хэдэн хариу мэдэгдэл (ж.нь бодит токен үүсгэхээс өмнө баримтыг илгээх шаардлагатай бол) үүсгэх ёстой бол шинэ асуулгын лавлагаа үүсгэж буцаана.

ЦБҮҮ-ийн эцсийн хариу мэдэгдлийг санаачлагч хүлээн авсны дараа асуулгын шинэ лавлагаа өгөхгүй.

Санаачлагч нь TCP-д суурилсан ЦБҮҮ-ийн шууд мэдэгдлийг хүлээн авагч руу илгээдэг. Хүлээн авагч нэгэн ижил мэдэгдэл хариу илгээдэг.

TCP-д суурилсан ЦБҮҮ-ийн шууд мэдэгдэл дараах зүйлсээс бүрдэнэ:

урт (32-bits), тэмдэглэл-flag (8-bits), утга (доор тодорхойлсон)

“Урт” хэмээх талбар нь мэдэгдлийн (мессеж) үлдэгдэл наймтын тоог агуулдаг (өөрөөр хэлбэл "утга"-ын наймтын тоон дээр нэгийг нэмсэн). Энэ протоколын 32 битийн бүх утгыг сүлжээний байтын дарааллаар зааж өгсөн болно.

Message name flag value
tsaMsg ’00’H DER-encoded TSA message
-- TSA message
pollRep ’01’H polling reference (32 bits),
time-to-check-back (32 bits)
-- poll response where no TSA message response ready; use polling
-- reference value (and estimated time value) for later polling
pollReq ’02’H polling reference (32 bits)
-- request for a TSA message response to initial message
negPollRep ’03’H ’00’H
-- no further polling responses (i.e., transaction complete)
partialMsgRep ’04’H next polling reference (32 bits),
time-to-check-back (32 bits),
DER-encoded TSA message
-- partial response (receipt) to initial message plus new polling
-- reference (and estimated time value) to use to get next part of
-- response
finalMsgRep ’05’H DER-encoded TSA message
-- final (and possibly sole) response to initial message
errorMsgRep ’06’H human readable error message
-- produced when an error is detected (e.g., a polling reference
-- is received which doesn’t exist or is finished with)

Гарч ирж болон мэдэгдэл дараах дараалалтай байна:

a) Эхний этгээд tsaMsg илгээж pollRep, negPollRep, partialMsgRep, юм уу finalMsgRep-ийн аль нэгийг хариу болгон хүлээж авна.

b) Эцсийн этгээд pollReq мэдэгдэл илгээж negPollRep, partialMsgRep, finalMsgRep, юм уу errorMsgRep-ийн аль нэгийг хариу болгон хүлээж авна.

" time-to-check-back -батлах хүртэлх хугацаа" параметр үзүүлэлт нь гарын үсэг зурагдаагүй 32 битийн бүхэл тоо байна. Энэ нь клиент программ төлөвийг дахин

шалгахын тулд хүлээх ЁСТОЙ хамгийн бага интервалыг секундээр илэрхийлдэг хугацаа юм.

Энэ нь эцсийн этгээд дараагийн pollReq илгээх ёстой хугацааг тооцоолох боломжийг олгодог.

3.4. HTTP-ээр дамжуулсан Цагийн бүрд гэлийн протокол

Энэ дэд хэсэгт HyperText Transfer Protocol-оор дамжуулан 2-р бүлэг болон Хавсралт D-д тодорхойлсон протоколыг солилцоход зориулсан ASN.1-шифрлэсэн мэдэгдлийг дамжуулах хэрэгслийг зааж өгсөн.

MIME хоёр объектыг дараах байдлаар тодорхойлсон.

Content-Type: application/timestamp-query

<<the ASN.1 DER-encoded Time-Stamp Request message>>

Content-Type: application/timestamp-reply

<<the ASN.1 DER-encoded Time-Stamp Response message>>

Эдгээр MIME объектыг WWW холбоосоор дамжуулан нийтлэг HTTP-г боловсруулах ердийн механизм ашиглан илгээж, хүлээн авч болох бөгөөд цагийн бүрд гэлийн мэдэгдлийг энгийн браузер хөтөч болон серверийн хооронд дамжуулан тээвэрлэх боломжийг хангадаг.

Сервер хүчинтэй хүсэлт хүлээн авмагц application/timestamp-response төрлийн агуулгатай хариу өгөх юм уу HTTP-ийн алдаа заасан тухай хариу өгөх ЁСТОЙ.

4. Аюулгүй байдлын асуудлууд

Энэ баримт бичиг бүхэлдээ аюулгүй байдлын асуудалд хамааралтай. ЦБҮҮ-ийн үйлчилгээг зохиомжлох үед цагийн бүрд гэлийн токений хүчинтэй байдал эсвэл "итгэлцэл"-д нөлөөлөх дараах хүчин зүйлсийг тодорхойлсон.

1. ЦБҮҮ-ийг цаашид ашиглахгүй байгаа, гэхдээ ЦБҮҮ-ийн хувийн түлхүүр задраагүй, асуудалд ороогүй тохиолдолд гэрчилгээ олгох байгууллагын гэрчилгээг хүчингүй болгох ЁСТОЙ. ЦБҮҮ-ийн хүчингүй болсон гэрчилгээтэй холбоотой reasonCode өргөтгөл хүчингүй гэрчилгээний жагсаалтад (ХГЖ) байгаа бол түүнийг unspecified (0), affiliationChanged (3), superseded (4) юм уу cessationOfOperation (5) гэж тохируулна. Энэ тохиолдолд цаашдаа аль ч үед хамаарах түлхүүрээр гарын үсэг зурсан токен хүчингүйд тооцогдох боловч хүчингүй болгох хугацаанаас өмнө үүсгэсэн токен хүчинтэй хэвээр үлдэнэ. Хэрэв ЦБҮҮ-ээс хүчингүй болгосон гэрчилгээтэй холбоотой reasonCode өргөтгөл ХГЖ-ын бичлэгт байхгүй бол тухайн түлхүүрээр гарын үсэг зурсан бүх токеныг хүчингүй гэж үзнэ. Тиймээс reasonCode өргөтгөлийг ашиглахыг зөвлөдөг.

2. TSA хувийн түлхүүр алдагдсан тохиолдолд хамаарах бүх гэрчилгээг хүчингүй болгох ЁСТОЙ. Энэ тохиолдолд ЦБҮҮ-ийн хүчингүй болгосон гэрчилгээтэй холбоотой reasonCode өргөтгөл ХГЖ-ын оруулгын өргөтгөлүүдэд байх юм уу байхгүй байж болно. Хэрэв байгаа бол keyCompromise (1) гэж тохируулагдсан байх ёстой. Тухайн хувийн түлхүүрийг ашиглан ЦБҮҮ-ээс гарын үсэг зурсан аливаа токенд цаашид итгэх боломжгүй. Энэ шалтгааны улмаас ЦБҮҮ-ийн хувийн түлхүүр задрах,

алдагдах боломжийг багасгахын тулд түүнийг аюулгүй байдлын зохих арга хэмжээний дагуу, хяналтын доор хамгаалах зайлшгүй шаардлагатай. Хувийн түлхүүр задарсан, алдагдсан тохиолдолд ЦБҮҮ-ээс үүсгэсэн бүх токены аудит хяналтын журналаас жинхэнэ болон хуурамч токенийг ялгах арга хэрэгсэл гаргаж өгч БОЛНО. Асуудлыг шийдэх өөр нэг арга нь хоёр өөр ЦБҮҮ-ийн олгосон хоёр өөр токен байх болно.

3. Хангалттай удаан хугацаанд үйлчлэх боломжийг хангахын тулд ЦБҮҮ-ийн гарын үсэг зурах түлхүүр нь хангалттай урт байх ЁСТОЙ. Үүнийг хангаж чадсан ч түлхүүр дуусах хугацаа байна. Тиймээс, ЦБҮҮ-ийн гарын үсэг зурсан аливаа токенд сүүлд нь дахин цагийн бүрд гэл - тамга (хуучин ХГЖ-ын жинхэнэ хуулбар байгаа бол) дарах юм уу нотариатаар гэрчлүүлэх (хэрэв дээрх байхгүй бол) замаар ЦБҮҮ-ийн гарын үсэгт итгэх итгэлийг сэргээх ЁСТОЙ. Энэхүү итгэлцлийг хангахын тулд цагийн бүрд гэлийн токенийг нотлох баримт бүрд гэх байгууллагад хадгалж болно.

4. Зөвхөн нэг удаагийн дугаар ашигладаг, орон нутгийн цаг ашигладаггүй клиент программ нь хариу хүлээхэд шаардлагатай цаг хугацааны талаар анхаарах ЁСТОЙ. "Дунд нь байгаа хүн - man-in-the-middle" халдлага нь саатал үүсгэж болзошгүй. Тиймээс хүлээн зөвшөөрөгдөх хугацаанаас илүү хугацаа шаардагдаж буй TimeStampResp-ийг сэжигтэй гэж тооцох ХЭРЭГТЭЙ. Энэхүү баримт бичигт тусгасан тээвэрлэлтийн арга бүр саатлын өөр өөр шинж чанартай байдаг тул хүлээн зөвшөөрөгдөх хугацаа нь ашиглаж буй тээвэрлэлтийн тодорхой арга, түүнчлэн хүрээлэн буй орчны бусад хүчин зүйлээс хамаарна.

5. Хэрэв өөр өөр этгээд ижил хэш алгоритмыг ашиглан нэг өгөгдөлд цагийн бүрд гэл хийлгэсэн (тамга даруулсан) юм уу, эсхүл нэг этгээд нэг өгөгдөлд олон токен авсан бол үүсгэсэн цагийн бүрд гэлийн токенууд нэгэн ижил мэдэгдэл-мессежний дардас агуулна; үүний үр дүнд эдгээр цагийн бүрд гэлийн токенд хандах боломжтой ажиглагч тухайн цагийн бүрд гэл нь нэгэн ижил үндсэн өгөгдөлд хамаарч болно гэж дүгнэх боломжтой.

6. Нэгэн ижил хэш алгоритм болон утгыг агуулсан хүсэлтийг санамсаргүй эсвэл санаатайгаар дахин дахин гаргах тохиолдол байж болно. Сүлжээний дамжуулах элементүүдэд асуудал үүссэний улмаас хүсэлтийн мэдэгдлийн олон хуулбарыг ЦБҮҮ-д илгээсэн тохиолдолд санамсаргүй давталт үүсдэг. Дунд нь байгаа этгээд ЦБҮҮ-ийн хууль ёсны хариуг дахин сэргээх үед зориудаар дахин хүсэлт гаргасан тохиолдол үүсэж болно. Эдгээр нөхцөл байдлыг илрүүлэхийн тулд хэд хэдэн аргыг ашиглаж болно. Нэг удаагийн дугаар ашиглах нь давтсан хүсэлтийг илрүүлэх боломжийг олгодог тул түүнийг ашиглахыг ЗӨВЛӨЖ байна. Өөр нэг боломж нь хүсэлт гаргагч тухайн цагийн хүрээнд илгээсэн бүх хэшийг санаж тогтоох замаар орон нутгийн цаг болон хөдөлж буй цагийн хүрээг хоёуланг нь ашиглах явдал юм. Хүсэлт гаргагч хариулт хүлээн авах үедээ хариу өгөх хугацаа нь тухайн цагийн хүрээнд багтаж байгаа эсэх, мөн тухайн цагийн хүрээнд зөвхөн нэг хэш утга орж ирсэн гэдгийг баталгаажуулдаг. Хэрэв тухайн цагийн хүрээнд ижил хэш утга нэгээс олон удаа байвал хүсэлт гаргагч нь нэг удаагийн дугаар ашиглах юм уу эсвэл тухайн цагийн хүрээнд ижил хэш утга нэг удаа гарч ирэх хүртэл өөрчлөгдөхийг хүлээх боломжтой.

5. Оюуны өмчийн эрх

IETF (Internet Engineering Task Force) энэхүү баримт бичигт дурдсан технологийг хэрэгжүүлэх, ашиглахтай холбоотой оюуны өмчийн болон бусад эрхийн хүчинтэй байдал, хамрах хүрээний талаар болон энэ эрхтэй хамааралтай аливаа лицензийн хүртээмжтэй байдлын талаар ямар нэг байр суурь баримтлахгүй; түүнчлэн аливаа ийм эрхийг тодорхойлох хүчин чармайлт гаргаагүй. Стандартыг мөшгөн ажиглах болон стандарттай холбоотой баримт бичиг дахь оюуны өмчийн эрхийн талаарх IETF-ийн журмын тухай мэдээллийг BCP-11-ээс үзэж болно. Нийтлэхэд бэлэн болсон оюуны өмчийн эрхийн тухай мэдэгдлийн хуулбар, лицензийн хүртээмжтэй байдлын аливаа баталгаа, эсхүл энэ тодорхойлолтыг хэрэгжүүлэгч болон хэрэглэгч ийм оюуны өмчийн эрхийг ашиглах нийтлэг лиценз олж авах оролдлогын үр дүнг IETF-ийн нарийн бичгийн дарга нарын газраас авч болно.

IETF нь энэхүү стандартыг хэрэгжүүлэхэд шаардагдаж болох технологитой хамааралтай аливаа зохиогчийн эрх, патент, патентын мэдүүлэг болон бусад өмчийн эрхэд дурын сонирхогч тал анхаарлаа хандуулахыг санал болгож байна. Энэ талын мэдээллийг IETF-ийн Гүйцэтгэх захиралд илгээнэ үү.

Одоогийн байдлаар цагийн бүрд гэлтэй холбоотой, он цагийн дарааллаар жагсаасан АНУ-ын дараах найман (8) патент байгаа гэдгийг зохиогчид мэдэж байна. Энэ нь бүрэн дүүрэн жагсаалт биш байж магадгүй. Бусад патентууд БАЙЖ болохоос гадна шинээр олгогдож болно. Энэ жагсаалтыг мэдээллийн зорилгоор өгч байгаа болно; Өнөөдрийг хүртэл IETF-д энэхүү баримт бичигт тусгагдсан аливаа тодорхойлолттой хамааралтай оюуны өмчийн эрхийн талаар мэдэгдэл ирээгүй байна. Энэ нөхцөл байдал өөрчлөгдсөн тохиолдолд хандаж бүрд гүүлсэн оюуны өмчийн эрхийн онлайн жагсаалтаас (IETF - ийн Оюуны өмчийн эрхийн талаарх мэдэгдлийн хуудас) одоогийн төлөвийг харж болно.

Энэхүү протоколыг хэрэгжүүлж буй этгээд өөрөө патентын хайлт хийж, түүнийг хэрэгжүүлэхэд хүндрэл, саад байгаа эсэхийг тодорхойлох ХЭРЭГТЭЙ.

Энэхүү протоколыг хэрэглэж буй этгээд өөрөө патентын хайлтыг хийж, энэ стандартыг ашиглахад ямар нэгэн хүндрэл, саад байгаа эсэхийг тодорхойлох ХЭРЭГТЭЙ.

5,001,752 Public/Key Date-Time Notary Facility Filing date:
October 13, 1989
Issued: March 19, 1991 Inventor:
Addison M. Fischer

5,022,080 Electronic Notary Filing date:
April 16, 1989
Issued: June 4, 1991
Inventors: Robert T. Durst, Kevin D. Hunter

5,136,643 Public/Key Date-Time Notary Facility Filing date:

December 20, 1990
Issued: August 4, 1992
Inventor: Addison M. Fischer
Note: This is a continuation of patent # 5,001,752.)

5,136,646 Digital Document Time-Stamping with Catenate Certificate Filing date:
August 2, 1990
Issued: August 4, 1992
Inventors: Stuart A. Haber, Wakefield S. Stornetta Jr. (assignee) Bell
Communications Research, Inc.,

5,136,647 Method for Secure Time-Stamping of Digital Documents Filing date:
August 2, 1990
Issued: August 4, 1992
Inventors: Stuart A. Haber, Wakefield S. Stornetta Jr. (assignee) Bell
Communications Research, Inc.,

5,373,561 Method of Extending the Validity of a Cryptographic Certificate
Filing date: December 21, 1992
Issued: December 13, 1994
Inventors: Stuart A. Haber, Wakefield S. Stornetta Jr. (assignee) Bell
Communications Research, Inc.,

5,422,953 Personal Date/Time Notary Device Filing
date: May 5, 1993
Issued: June 6, 1995 Inventor:
Addison M. Fischer

5,781,629 Digital Document Authentication System Filing date:
February 21, 1997
Issued: July 14, 1998
Inventor: Stuart A. Haber, Wakefield S. Stornetta Jr. (assignee)
Surety Technologies, Inc.,

6. Ном зүй

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol, Version 1.0", RFC 2246, January 1999.

[RFC2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure, Certificate Management Protocols", RFC 2510, March 1999.

[RFC2459] Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile", RFC 2459, January 1999.

[CMS] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[DSS] Digital Signature Standard. FIPS Pub 186. National Institute of Standards and Technology. 19 May 1994.

[ESS] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[ISONR] ISO/IEC 10181-5: Security Frameworks in Open Systems. Non-Repudiation Framework. April 1997.

[MD5] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[SHA1] Secure Hash Standard. FIPS Pub 180-1. National Institute of Standards and Technology. 17 April 1995.

ХАВСРАЛТ А – CMS ашиглан гарын үсэгт цагийн бүрд гэл хийх

Цагийн бүрд гэлийн нэг гол хэрэглээ нь тоон гарын үсгийг тодорхой хугацаанаас өмнө үүсгэсэн гэдгийг нотлохын тулд тоон гарын үсэгт цагийн бүрд гэл хийх (тамга дарах) байдаг. Хамаарах нийтийн түлхүүрийн гэрчилгээг хүчингүй болгосон тохиолдолд гэрчилгээг хүчингүй болгосон өдрөөс өмнө эсвэл дараа нь гарын үсгийг үүсгэсэн эсэхийг баталгаажуулагч хэрхэн мэдэх вэ гэдэг асуудал гарч ирдэг. Цагийн бүрд гэлийг хадгалахад тохиромжтой газар нь тэмдэггүй шинжүүдийн хэлбэртэй [CMS] бүтэц байдаг.

Энэхүү хавсралтад тоон гарын үсэгт цагийн бүрд гэл хийхэд ашиглагдаж болох тоон гарын үсгийн цагийн бүрд гэлийн шинжүүдийг тодорхойлсон.

Дараах объектын адилтгагч нь гарын үсгийн цагийн бүрд гэлийн шинжүүдийг тодорхойлдог:

id-aa-timeStampToken OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) aa(2) 14 }

Гарын үсгийн цагийн бүрд гэлийн шинжийн утга нь ASN.1 type
SignatureTimeStampToken:
SignatureTimeStampToken ::= TimeStampToken байна.

TimeStampToken доторх messageImprint талбарын утга нь гарын үсэг зурсан өгөгдөлд зориулсан SignerInfo доторх гарын үсгийн талбарын утгын хэш байх ёстой.

ХАВСРАЛТ В – Тодорхой цаг мөчид гарын үсэг зурах

Бид энэхүү цагийн бүрд гэлийн нийтлэг үйлчилгээг ашиглах боломжит жишээг толилуулж байна. Энэ үйлчилгээ нь тодорхой цаг мөчид гарын үсэг зурдаг бөгөөд тухайн гэрчилгээний төлөвийн мэдээллийг (жишээ нь, ХГЖ) тухайн гарын үсэгт суурилан шалгаж байх ЁСТОЙ. Энэхүү хэрэглээний программ нь тоон гарын үсгийн механизм ашиглан үүсгэсэн нотлох баримттай хамт ашиглагдах зориулалттай.

Гарын үсгийг зөвхөн үл татгалзах шинжийг хангах бодлогын дагуу баталгаажуулах боломжтой. Энэ бодлого нь далд юм уу ил тод БАЙЖ болно (тухайлбал, гарын үсэг зурагчийн гаргаж өгсөн нотолгоонд тусгасан). Түүнчлэн үл татгалзах шинжийг хангах бодлого нь тоон гарын үсэг үүсгэхэд ашигласан гарын үсгийн түлхүүр алдагдсан, эрсдэлд орсныг гарын үсэг зурагч мэдээлж болох эцсийн хугацааг зааж өгч болно. Тиймээс энэхүү эцсийн хугацаа дуусахаас өмнө гарын үсэг хүчинтэй байх баталгаа байхгүй.

Тоон гарын үсгийг баталгаажуулахад дараах үндсэн аргуудыг ашиглаж болно:

A) Гарын үсгийг үүсгэснээс хойш удалгүй (ж.нь., хэдэн минут юм уу цагийн дотор) цагийн бүрд гэлийн мэдээллийг олж авах.
   1) Гарын үсгийг Цагийн бүрд гэлийн үйлчилгээ үзүүлэгчид (ЦБҮҮ) гаргаж өгнө. ЦБҮҮ энэ гарын үсгээр үүсгэсэн TimeStampToken (ЦБТ)-ийг буцаан илгээнэ.
   2) Хүсэлт гаргагч TimeStampToken зөв байгаа эсэхийг шалган баталгаажуулна.

B) Үүний дараа тоон гарын үсгийн хүчинтэй эсэхийг дараах замаар шалгаж болно:
   1) Цагийн бүрд гэлийн токенийг өөрийг нь шалгах ЁСТОЙ-оос гадна зурагчийн гарын үсэгт хамаарч байгаа гэдгийг шалгах ЁСТОЙ.
   2) ЦБҮҮ-ийн цагийн бүрд гэлийн токенд тусгасан огноо, хугацааг гаргаж авах ЁСТОЙ.
   3) Зурагчийн ашигласан гэрчилгээг адилтгаж, гаргаж авах ЁСТОЙ.
   4) ЦБҮҮ-ийн тусгасан огноо, цаг нь зурагчийн гэрчилгээний хүчинтэй хугацааны дотор байх ЁСТОЙ.
   5) Гэрчилгээг хүчингүй болгосон талаар мэдээллийг цагийн бүрд гэл хийсэн огноо, хугацааны дагуу гаргаж авах ЁСТОЙ.
   6) Гэрчилгээг хүчингүй болгосон бол хүчингүй болгосон огноо, хугацаа нь ЦБҮҮ-ийн тусгасан огноо, хугацаанаас хойно байх ёстой.

Энэ бүх нөхцөл хангагдсан бол тоон гарын үсгийг хүчинтэй гэж зарлана.

ХАВСРАЛТ С: 1988 Синтакс ашигласан ASN.1 модуль

```
PKIXTSP {iso(1) identified-organization(3) dod(6) internet(1)

    security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-tsp(13)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

      Extensions, AlgorithmIdentifier
      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)}
      GeneralName 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)}
      ContentInfo FROM CryptographicMessageSyntax {iso(1)
      member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
      smime(16) modules(0) cms(1)}
      PKIFreeText FROM PKIXCMP {iso(1) identified-organization(3)
      dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-cmp(9)} ;

                                        -- Locally defined OIDs --

-- eContentType for a time-stamp token

1 id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

-- 2.4.

TimeStampReq ::= SEQUENCE {

      version INTEGER { v1(1) },
      messageImprint MessageImprint,
      --a hash algorithm OID and the hash value of the data to be
      --time-stamped
      reqPolicy TSAPolicyId OPTIONAL,
      nonce INTEGER OPTIONAL,
      certReq BOOLEAN DEFAULT FALSE,
      Extensions OPTIONAL }

MessageImprint ::= SEQUENCE extensions [0] IMPLICIT {

      hashAlgorithm AlgorithmIdentifier,
      hashedMessage OCTET STRING }

TSAPolicyId ::= OBJECT IDENTIFIER


-- 2.4.2

TimeStampResp ::= SEQUENCE {
```

```
        status PKIStatusInfo,
        timeStampToken TimeStampToken OPTIONAL }


-- The status is based on the definition of status
-- in section 3.2.3 of [RFC2510]

PKIStatusInfo ::= SEQUENCE {

        status PKIStatus,
        statusString PKIFreeText OPTIONAL,
        failInfo PKIFailureInfo OPTIONAL }


PKIStatus ::= INTEGER {

        granted (0),
        -- when the PKIStatus contains the value zero a TimeStampToken, as
        requested, is present.
        grantedWithMods (1),
        -- when the PKIStatus contains the value one a TimeStampToken,
        with modifications, is present.
        rejection (2),
        waiting (3),
        revocationWarning (4),
        -- this message contains a warning that a revocation is
        -- imminent
        revocationNotification (5)
        -- notification that a revocation has occurred }
        -- When the TimeStampToken is not present
        -- failInfo indicates the reason why the
        -- time-stamp request was rejected and
        -- may be one of the following values.


PKIFailureInfo ::= BIT STRING {

        badAlg (0),
        -- unrecognized or unsupported Algorithm Identifier
        badRequest (2),
        -- transaction not permitted or supported
        badDataFormat (5),
        -- the data submitted has the wrong format
        timeNotAvailable (14),
        -- the TSA's time source is not available
        unacceptedPolicy (15),
        -- the requested TSA policy is not supported by the TSA.
        unacceptedExtension (16),
        -- the requested extension is not supported by the TSA.
        addInfoNotAvailable (17)
        -- the additional information requested could not be understood
        -- or is not available
        systemFailure (25)
        -- the request cannot be handled due to system failure }
```

```
TimeStampToken ::= ContentInfo

    -- contentType is id-signedData as defined in [CMS]
    -- content is SignedData as defined in([CMS])
    -- eContentType within SignedData is id-ct-TSTInfo
    -- eContent within SignedData is TSTInfo


TSTInfo ::= SEQUENCE {

    version INTEGER { v1(1) },
    policy TSAPolicyId,
    messageImprint MessageImprint,
    -- MUST have the same value as the similar field in
    -- TimeStampReq
    serialNumber INTEGER,
    -- Time-Stamping users MUST be ready to accommodate integers
    -- up to 160 bits.
    genTime GeneralizedTime,
    accuracy Accuracy OPTIONAL,
    ordering BOOLEAN DEFAULT FALSE,
    nonce INTEGER OPTIONAL,
    -- MUST be present if the similar field was present
    -- in TimeStampReq. In that case it MUST have the same value.
    tsa [0] GeneralName OPTIONAL,
    extensions [1] IMPLICIT Extensions OPTIONAL }


Accuracy ::= SEQUENCE {

                    seconds         INTEGER             OPTIONAL,
                    millis      [0] INTEGER (1..999)    OPTIONAL,
                    micros      [1] INTEGER (1..999)    OPTIONAL }


END
```

ХАВСРАЛТ D: Цагийн бүрд гэлд хандах хандалтын тодорхойлогчид

Энэ хавсралтад "son-of-RFC2459"-д тодорхойлогдсон SIA (Subject Information Access) өргөтгөлд суурилсан өргөтгөлийг тайлбарласан.

Энэхүү баримт бичгийг нийтлэх үед "son-of-RFC2459" хараахан гараагүй байгаа тул түүний тайлбарыг мэдээллийн хавсралтад оруулсан болно. Дараа нь энэ хавсралтын агуулгыг "son-of-RFC2459" баримт бичигт багтаах учир энэ хавсралт шаардлагагүй болно. Энэ баримт бичгийн ирээдүйд гарах хувилбарт энэ хавсралтыг орхих бөгөөд "son-of-RFC2459" баримт бичгийг шууд эшилнэ.

ЦБҮҮ-тэй холбогдох аргыг зөөвөрлөхийн (дамжуулах) тулд ЦБҮҮ-ийн гэрчилгээнд Subject Information Access (SIA) өргөтгөл (son of RFC2459) агуулагдаж БОЛНО. Энэ өргөтгөлийн accessMethod талбар нь id-ad-timestamping-ийн OID -ийг агуулсан байх ЁСТОЙ: Объектын дараах адилтгагч (танигч) нь цагийн бүрд гэлд хандах хандалтын тодорхойлогчдыг адилтгадаг.

id-ad-timeStamping OBJECT IDENTIFIER ::= {iso(1)
identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
ad (48) timestamping (3)}

AccessLocation талбарын утга нь ЦБҮҮ-д хандахад ашигладаг тээвэрлэлтийг (жишээ нь, HTTP) тодорхойлдог бөгөөд тээвэрлэлттэй хамааралтай бусад мэдээллийг (жишээ нь, URL) агуулж болно.