МОНГОЛ УЛСЫН СТАНДАРТ

Ангилалтын код 5280

Интернэт X.509 Нийтийн Түлхүүрийн Дэд бүтцийн Гэрчилгээ ба Хүчингүй Гэрчилгээний Жагсаалт (ХГЖ)-ийн профайл	**MNS xxxx**
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	**RFC 5280**

Хураангуй

Энэ санамж нь X.509 хувилбар 3 гэрчилгээ болон X.509 хувилбар 2 Хүчингүй гэрчилгээний жагсаалт (ХГЖ) интернэтэд ашиглах боломжтойгоор хэлбэржүүлнэ. Энэхүү арга зам болон загварын тоймыг танилцуулга бүлэгт оруулсан болно. X.509 хувилбар 3 гэрчилгээний форматыг Интернэтийн нэрийн маягтуудын формат болон утгазүйн талаарх нэмэлт мэдээллийг дэлгэрэнгүй тодорхойлсон. Стандарт гэрчилгээний өргөтгөлүүдийг тайлбарласан ба Интернэтэд-зориулсан хоёр өргөтгөлийг тодорхойлсон. Шаардлагатай гэрчилгээний өргөтгөлийн багцыг зааж өгсөн. X.509 хувилбар 2 ХГЖ форматыг стандарт болон интернэтэд зориулсан өргөтгөлүүдийн хамт дэлгэрэнгүй тайлбарласан болно. X.509 гэрчилгээний шатлалыг шалгахад зориулсан алгоритмыг тайлбарлав. ASN.1 модуль болон жишээг хавсралтуудад оруулсан болно.

1. Танилцуулга

Энэ тодорхойлолт нь Интернэт дэх X.509 Нийтийн Түлхүүрийн Дэд Бүтэц (НТДБ)- д зориулсан стандартуудын бүлийн нэг юм.

Энэхүү тодорхойлолт нь Интернэт НТДБ-д зориулсан гэрчилгээнүүд болон Хүчингүй гэрчилгээний жагсаалт (ХГЖ)-уудын формат болон семантикуудыг тодорхойлно. Процедруудыг Интернэт орчин дахь гэрчилгээний шатлалыг боловсруулахад зориулан тодорхойлов. Төгсгөлд нь ASN.1 модулиуд бүх өгөгдлийн бүтцийн тодорхойлолт эсвэл эшлэл /хамаарал- д зориулан хавсралтуудаар хангасан.

Бүлэг 2-т Интернэтийн НТДБ-ийн шаардлагуудыг тодорхойлсон ба энэ баримт бичгийн хүрээний нөлөөллийг таамаглав. Бүлэг 3-т архитектурт загварыг үзүүлсэн ба өмнөх IETF, ISO, IEC, ITU-T стандартуудтай харилцан хамаарлын тодорхойлсон. Жишээлбэл энэ баримт бичгийн IETF-ийн НТДБ

тодорхойлолтууд болон ISO/IEC/ITU-T X.509 баримт бичгүүдтэй харилцан хамаарлыг тодорхойлсон.

Бүлэг 4-т X.509 хувилбар 3 гэрчилгээг тодорхойлсон ба Бүлэг 5-т X.509 хувилбар 2 ХГЖ тодорхойлсон. Профайлууд нь Интернэт НТДБ-д ашиглаж болох ISO/IEC/ITU-T ба ANSI өргөтгөлүүдийг адилтгагчийг багтаана. Профайлуудыг хамгийн сүүлийн ISO/IEC/ITU-T стандартуудад хэрэглэсэн 1997 ASN.1 өгүүлбэрзүйгээс илүү 1988 Abstract Syntax Notation One (ASN.1)- д үзүүлсэн.

Бүлэг 6-т гэрчилгээний шатлалыг шалгах үйл ажиллагааг багтаасан. Тэдгээр үйл ажиллагааг ISO/IEC/ITU-T тодорхойлолтууд дээр үндэслэсэн. Хэрэгжүүлэлтэд ижил үр дүн гаргаж авах ШААРДЛАГАТАЙ боловч заасан үйл ажиллагаа ашиглах ШААРДЛАГАТАЙ биш.

Нийтийн түлхүүрийн материалууд ба тоон гарын үсгийн шифрлэх болон таних процедурыг [RFC3279],[RFC4055],[RFC4491]-д тодорхойлсон. энэхүү тодорхойлолтын хэрэгжүүлэлтэд ямар нэгэн жишээ крифтографийн алгоритмууд хэрэглэхийг шаардахгүй. Гэхдээ хэрэгжүүлэлтийн нийцүүлэхдээ [RFC3279], [RFC4055], [RFC4491]- д тодорхойлсон нийтийн түлхүүрийн материалууд ба тоон гарын үсгүүдийг олж тогтоох ба шифрлэх алгоритмуудыг ЗААВАЛ хэрэглэнэ.

Эцэст нь гурван хавсралтууд хэрэгжүүлэгчдийг тусламжаар хангана. Хавсралт А нь бүх ANS.1 бүтцийг тодорхойлсон болон энэхүү тодорхойлолтын эшлэлүүдийг багтаасан. Дээр дурдсан материалуудыг 1988 ASN.1-д үзүүлсэн. Хавсралт В энэхүү тодорхойлолтуудтай хамт хэрэглэгдэх ASN.1 тэмдэглэгээний танил бус өвөрмөц атрибутуудын тэмдэглэлүүдийг агуулна. Хавсралт С нь ХГЖ-ийг нийцүүлэх ба гэрчилгээг нийцүүлэх жишээнүүдийг агуулна.

Энэ тодорхойлолт хоцрогдсон [RFC3280]. RFC 3280-ийн ялгаа нь доорх байдлаар нэгтгэн дүгнэв.

- Бүлэг 7-т олон улсын чанартай домэйн нэрс, олон улсын чанартай нөөцийн таних тэмдэг (ОУЧТТ), онцолсон нэрсийг харьцуулах болон шифрлэхэд зориулсан дүрмүүдийн хамт олон улсын чанартай нэрсийг дэмжих нэмэгдлийг тодорхойлсон. Эдгээр дүрмүүдийг [RFC3490],[RFC3987],[RFC4518] багтсан одоогийн RFCs-д харьцуулсан дүрмүүдийн байгуулагдсантай нийцсэн.
- Бүлэг 4.1.2.4 ба 4.1.2.6- т [RFC4630]-д заасан уламжлалт текст шифрлэх схемүүдийг үргэлжлүүлэн ашиглах нөхцөлийг тусгасан болно.

Байгуулагдсан НТДБ-ийг ашиглаж байгаа газарт UTF8String-рүү шилжих нь нэрийн хязгаарлалтын буруу боловсруулалт эсвэл нэрийн гинжлэлтийн алдаанууд дээр суурилсан Үйлчилгээ цуцлах халдлага (DoS)- ийн шалтгаан болж болзошгүй.

- RFC3280-ийн 4.2.1.4-т тодорхойлсон privateKeyUsagePeriod гэрчилгээний өргөтгөлийн хэрэглээ хуучирсан учир устгасан. Энэ ISO стандартын өргөтгөлийн Интернэт НТДБ дахь хэрэглээнд хуучирсан, зөвлөхгүй аль ч биш юм.
- Бүлэг 4.2.1.5-д бодлогын зураглалын өргөтгөлийг чухал гэж тэмдэглэхийг зөвлөж байна. RFC 3280 нь бодлогын зураглалын өргөтгөлийг чухал гэж тэмдэглэх шаарддаг.
- Бүлэг 4.2.1.11-д бодлогын хязгаарлалтын өргөтгөлийг чухал гэж тэмдэглэхийг шаардана. RFC 3280 нь бодлогын хязгаарлалтын өргөтгөлийг чухал эсвэл чухал бус гэж тэмдэглэхийг зөвшөөрсөн.
- Байгууллагын мэдээлэлд хандах (БМХ) ХГЖ өргөтгөлийг [RFC43325]- д заасан дагуу 5.2.7-р Бүлэг болгон нэмсэн.
- Бүлэг 5.2 ба 5.3-д танигдаагүй ХГЖ өргөтгөлүүдийг зохицуулах, ХГЖ-ийн оруулгын өргөтгөлүүдийн дүрмүүдийг тус тус тодруулна.
- RFC 3280-ын 5.3.2-д тодорхойлсон holdInstructionCode ХГЖ оруулгын өргөтгөлийг хассан .
- Бүлэг 6- т заасан шатлалыг шалгах алгоритм нь гэрчилгээний хэлхээн дэх гэрчилгээжүүлэх бодлогын өргөтгөлүүдийн чухал байдлыг хянахаа больсон. RFC 3280-д энэ мэдээллийг итгэмжлэгдсэн тал руу буцаасан.
- Аюулгүй байдлын анхаарах зүйл бүлэг нь ХГЖ түгээлтийн цэгүүд дэх https эсвэл ижил төстэй схемүүдийн ашиглалт, байгууллагын мэдээлэлд хандах эсвэл субъект мэдээллийн хандалтын өргөтгөлүүдээс үүсэх дугуй хамаарлын эрсдэлт хаяглагдсан.
- Аюулгүй байдлын талаар анхаарах бүлэг нь нэрийн тодорхой бус байдалтай холбоотой эрсдэлүүдийг авч үздэг.
- Аюулгүй байдлын асуудал бүлэгт ГОБ-ийн үйлдэлд өөрчлөлт оруулах дохио өгөх үйл ажиллагаанд зориулан RFC 4210 стандартыг иш татсан болно.

Хавсралт А дахь ASN.1 модулиуд нь RFC 3280-аас өөрчлөгдөөгүй бөгөөд ub-emailaddress-length 128-аас 255 болж PKCS #9 [RFC2985]-тай ижилсүүлэх

зорилготойгоор өөрчлөгдсөн.

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.

2. Шаардлагууд ба Таамаглалууд

Энэхүү техникийн тодорхойлолтын зорилго нь X.509 технологийг хэрэглэхийг хүсэж байгаа нийгэмлэгүүдэд зориулсан Интернэтийн программууд хамт X.509 гэрчилгээнүүдийн хэрэглэхийг хөнгөвчлөх профайлыг хөгжүүлэх юм. Ийм программуудад WWW, цахим шуудан, хэрэглэгч баталгаажуулалт, IPSec байж байна. X.509 гэрчилгээг ашиглахад учирч буй зарим саад бэрхшээлийг арилгахын тулд энэхүү баримт бичиг нь гэрчилгээний удирдлагын системүүдийн хөгжүүлэлт, хэрэглээний хэрэгслүүдийн хөгжүүлэлт, бодлогоор тогтоосон харилцан ажиллах чадвар зэргийг хурдасгах профайлыг тодорхойлно.

Зарим нийгэмлэгүүд профайлыг нэмэлт зөвшөөрөл, баталгаа, эсвэл үйл ажиллагааны шаардлагууд бүхий орчин эсвэл тусгай программын домэйнүүдийн шаардлагуудад нийцүүлэн нэмэлт хийх эсвэл солих шаардлагатай болно. Хэдий тийм боловч үндсэн программуудад зориулан байнга хэрэглэгддэг шинж чанаруудын нийтлэг төлөөллийг программ хөгжүүлэгчид шаардлагатай мэдээллийг тодорхой гэрчилгээ эсвэл гэрчилгээ хүчингүй болгох жагсаалт ХГЖ-ийн гаргагч/олгогчийг харьцуулахгүйгээр олж авч чадна гэж тодорхойлсон.

Гэрчилгээний хэрэглэгч Тодорхой гэрчилгээ дэх нийтийн түлхүүртэй холбоотой Баталгаажуулалт эсвэл Үл татгалзах шинжийг (татгалзалгүй байдал) хангах үйлчилгээнд найдахын өмнө гэрчилгээ олгогч байгуулга ГОБ-аар үүсгэсэн гэрчилгээний бодлогыг хянах хэрэгтэй. Үүний тулд энэхүү стандарт хуулийн дагуу заавал биелүүлэх дүрэм эсвэл үүргүүдийг зөөж өгөхгүй.

Атрибутын гэрчилгээ гэх мэт нэмэлт зөвшөөрөл, атрибутын удирдлагын хэрэгслүүд гарч ирэхийн хэрээр гэрчилгээнд орсон баталгаажуулсан шинж чанаруудыг хязгаарлах нь зүйтэй. Эдгээр удирдлагын бусад хэрэгслүүд нь олон баталгаажуулсан шинж чанаруудыг дамжуулах илүү тохиромжтой аргуудыг өгч болно.

2.1. Холболтууд ба топологи

Гэрчилгээний хэрэглэгчид ба Ялангуяа аюулгүй цахим шуудангийн хэрэглэгчид

тэдгээрийн харилцааны/холболтын топологийн хувьд орчингуудын өргөн хүрээнд ажиллуулах болно. Энэ профайл өндөр зурвасын өргөн, бодит цагийн IP холболт, эсвэл өндөр холболтын боломжгүй байдлыг хэрэглэгчдийг дэмждэг. Нэмээд, профайл нь галт хана эсвэл бусад шүүлтүүрлэгдсэн харилцан холбоог зөвшөөрнө. Нэмж дурдахад, профайл нь галт хана эсвэл бусад шүүсэн харилцаа холбоо байхыг зөвшөөрдөг.

Энэ профайл нь X.500 директор систем [X.500] эсвэл Хөнгөн директор хандалтын протокол (LDAP) директор системийг [RFC4510] ашиглахыг тооцдоггүй. Профайл нь X.500 директор эсвэл LDAP директорыг ашиглахыг хориглодоггүй; Гэсэн хэдий ч гэрчилгээ, ХГЖ-ыг түгээх аливаа хэрэгслийг ашиглаж болно.

2.2. Хүлээн зөвшөөрөхүйц шалгуур

Интернэтийн нийтийн түлхүүрийн дэд бүтэц (НТДБ)-ийн зорилго нь тодорхойлогч, автоматжуулсан таних, баталгаажуулалт, хандалтын хяналт, зөвшөөрлийн функцүүдийн хэрэгцээг хангах явдал юм. Эдгээр үйлчилгээнд үзүүлэх дэмжлэг нь гэрчилгээнд агуулагдах атрибутууд болон бодлогын өгөгдөл, гэрчилгээний шатлалын хязгаарлалт зэрэг гэрчилгээ дахь туслах хяналтын мэдээллийг тодорхойлдог.

2.3. Хэрэглэгчийн хүлээлт

Интернэт НТДБ-ийн хэрэглэгчид нь үйлчлүүлэгчийн программ хангамжийг ашигладаг хүмүүс ба процессууд бөгөөд гэрчилгээнд нэрлэгдсэн субъектүүд юм. Эдгээр хэрэглээнд цахим шуудангийн уншигч, бичигч, WWW хөтөч ба WWW серверүүдэд зориулсан клиент, чиглүүлэгч доторх IPsec-ийн түлхүүр менежер орно. Энэхүү профайл нь эдгээр хэрэглэгчдийн ашигладаг платформуудын хязгаарлалт, хэрэглэгчдийн өөрсдийнх нь боловсронгуй байдал, анхаарал болгоомжтой байх хязгаарлалтыг хүлээн зөвшөөрдөг. Энэ нь хэрэглэгчийн тохиргооны хамгийн бага хариуцлага (жишээ нь, итгэмжлэгдсэн ГОБ түлхүүр, дүрэм), гэрчилгээ доторх платформ ашиглалтын тодорхой хязгаарлалт, хэрэглэгчийг олон хорлонтой үйлдлээс хамгаалдаг гэрчилгээний шатлалын хязгаарлалт, баталгаажуулалтын функцийг ухаалаг автоматжуулах программуудаар илэрдэг.

2.4. Администраторын хүлээлт

Хэрэглэгчийн хүлээлтийн нэгэн адил Интернэтийн НТДБ профайл нь ерөнхийдөө ГОБ-г ажиллуулдаг хүмүүсийг дэмжих бүтэцтэй байдаг. Администраторуудад хязгааргүй сонголтоор хангах нь ГОБ администраторын нарийн алдаа нь өргөн хүрээний буултад хүргэх магадлалыг нэмэгдүүлдэг.

Түүнчлэн, хязгааргүй сонголтууд нь ГОБ-ийн үүсгэсэн гэрчилгээг боловсруулж, шалгадаг программ хангамжийг ихээхэн хүндрүүлдэг.

3. Аргын тойм

Нийтийн түлхүүрийн дэд бүтэц ашиглаж байгаа X.509 (НТДБХ) техникийн тодорхойлолтуудаар таамагласан архитектурын загвар талаас дараах байдлаар хялбарчлан харуулсан.

Энэ загварын бүрдэл хэсгүүд нь:

төгсгөлийн зүйл: НТДБ гэрчилгээний хэрэглэгч ба/эсвэл гэрчилгээний субъект болох төгсгөлийн хэрэглэгчийн систем

ГОБ: гэрчилгээ олгогч байгуулга (ГОБ)

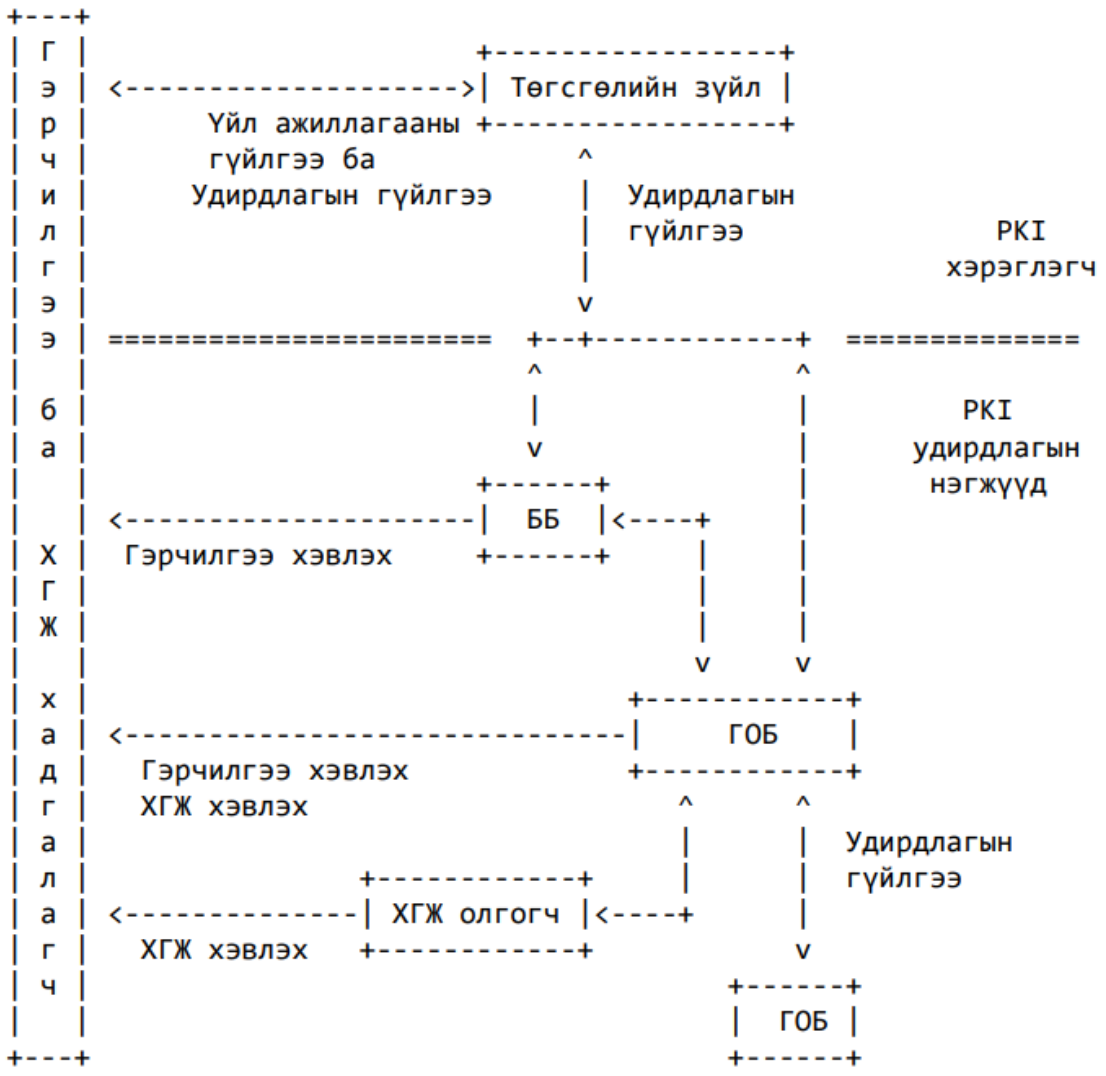
ББ: бүртгэлийн байгуулга (ББ), өөрөөр хэлбэл ГОБ-г төлөөлөх тодорхой менежментийн функцүүдтэй заавал биш систем

ХГЖ олгогч: ХГЖ-уудийг үүсгэх болон гарын үсэг зурах систем

Хадгалагч: гэрчилгээнүүд болон ХГЖ-ууд хадгалдаг тархсан системүүдийн цуглуулга эсвэл систем. Мөн тэдгээр гэрчилгээнүүд болон ХГЖ-уудыг төгсгөлийн зүйлсэд түгээх байдлаар үйлчилдэг.

ГОБ-ууд асуудалтай гэрчилгээнүүдийг хүчингүй төлөвийг таниулахыг хариуцна. Хүчингүй төлөвийн мэдээлэл нь Онлайн гэрчилгээний төлөв байдлын протокол (ОГТБП) [RFC2560], certificate revocation lists (ХГЖ) эсвэл бусад механизм ашиглан хангагдах байж болно. Ерөнхийдөө хүчингүй төлөвийн мэдээлэл нь ХГЖ ашиглан хангагдсан бол ГОБ нь мөн ХГЖ олгогч юм. Хэдий тийм боловч ГОБ асуудал гаргаж байгаа ХГЖ-уудыг ялгаатай зүйлүүдэд хариуцлагатайгаар төлөөлөх боломжтой.

Тэмдэглэл: Атрибутын эрх мэдлийг ХГЖ-уудын хэвлэлд ХГЖ олгогч төлөөлөхөөр бас сонгож болно.



Зураг 1 НТДБ-ийн нэгжүүд

3.1. X.509 хувилбар 3 гэрчилгээ

Нийтийн түлхүүрийн хэрэглэгчид шифрлэх эсвэл тоон гарын үсгийн механизмд ашиглагдах холбоотой түлхүүрийг нь зөв алсын субъект (хүн эсвэл систем)-ийн эзэмшдэг гэсэн итгэлтэй байх шаардлагатай. Энэхүү итгэлийг субъектүүдтэй холбох нийтийн түлхүүрийн утгууд буюу өгөгдлийн бүтцийн нийтийн түлхүүрийн гэрчилгээний хэрэглээгээр дамжуулан олж авна. Итгэмжлэгдсэн ГОБ нь гэрчилгээ бүрийг дижитал гарын үсэг зурснаар баталгаажуулна. ГОБ нь энэ мэдэгдлийг техникийн хэрэгслээр (харилцан хариу өгөх протоколоор дамжуулан эзэмшсэнийг нотлох), хувийн түлхүүрийн танилцуулга эсвэл субъектийн нотолгоонд тулгуурлаж болно. Гэрчилгээ нь түүний гарын үсэг

зурсан контентод заасан хязгаарлагдмал хүчинтэй үргэлжлэх хугацаатай байна. Учир нь гэрчилгээний гарын үсэг болон цагт гүйцэтгэх нь гэрчилгээ-ашиглах клиентээр тус тусдаа шалгагдаж болох ба гэрчилгээнүүд найдваргүй холболт болон серверийн системүүдээр тархсан, гэрчилгээ-ашиглах системүүд дэх найдваргүй хадгалуурт кешлэгдсэн/түр хадгалагдсан байж болно.

ITU-T X.509 (урьд өмнө CCITT X.509) эсвэл ISO/IEC 9594-8 нь X.500 директор зөвлөмжүүдийн нэг хэсэг болгож стандарт гэрчилгээний формат [X.509]- ыг тодорхойлон 1988 онд анх хэвлэгдсэн. 1988 оны стандартын гэрчилгээний форматыг хувилбар 1 формат гэж нэрлэгдэг. X.500- г 1993 онд шинэчлэх үед 2 талбар нэмэгдсэний үр дүнд хувилбар 2 формат болсон.

1993 онд хэвлэгдсэн Интернэтийн нууцлалын сайжруулсан шуудан (ИНСШ) RFCs нь X.509 хувилбар 1 гэрчилгээнүүд [RFC1422] дээр үндэслэн нийтийн түлхүүрийн дэд бүтцэд зориулсан тодорхойлолтуудыг багтаасан. RFC1422 хөгжүүлэх оролдлогуудаар олж авсан туршлага нь хувилбар 1 болон хувилбар 2 гэрчилгээний форматууд хэд хэдэн талаараа дутагдалтай байсныг тодорхой болгосон. Хамгийн чухал нь олон талбарууд ИНСШ дизайн болон хэрэгжүүлэх туршлага шаардлагатайг баталсан мэдээлэл зөөхөд шаардлагатай байсан. Хариуд нь эдгээр ISO/IEC, ITU-T, ANSI X9 хөгжүүлсэн X.509 хувилбар 3 гэрчилгээний формат гэсэн шинэ шаардлагууд гарсан. Хувилбар 3 формат нь нэмэлт өргөтгөлийн талбаруудад зориулсан заалтыг нэмснээр хувилбар 2 форматыг өргөтгөдөг. Ялангуяа өргөтгөлийн талбарын төрлүүд стандартуудад магадгүй тодорхойлогдох эсвэл дурын байгуулга эсвэл нийгэмлэгээр тодорхойлогдох болон бүртгэгдэх боломжтой. 1996 оны 6-р сард үндсэн хувилбар 3-ийн стандартчилал дууссан [X.509].

ISO/IEC, ITU-T, ANSI X9 нь Хувилбар 3 өргөтгөлийн [X.509], [X9.55] талбарт хэрэглэхэд зориулан стандартын өргөтгөлүүдийг мөн хөгжүүлсэн. Эдгээр өргөтгөлүүд субъектийг адилтгах нэмэлт мэдээлэл, гол атрибутын мэдээлэл, бодлогын мэдээлэл, гэрчилгээний шатлалын хязгаарлалт зэрэг өгөгдлийг зөөж чадна.

Хэдий тийм ч ISO/IEC, ITU-T, ANSI X9 стандартын өргөтгөлүүд нь тэдгээрийг хэрэглэх боломжоор маш өргөн. Интернэт хэрэглээнд зориулсан X.509 хувилбар 3 системүүдийн хэрэгжүүлэлтийг харилцан ажиллах боломжтойгоор хөгжүүлэхийн тулд Интернэтэд зориулсан тохируулсан X.509 хувилбар 3 өргөтгөлүүдийн хэрэглээнд зориулан зайлшгүй шаардлагатай профайлыг зааж өгөх шаардлагатай.

Энэхүү баримт бичгийн нэг зорилго нь Интернэт WWW, цахим шуудан, IPSec

аппликейшнуудад зориулсан профайлыг тодорхойлох юм. Нэмэлт шаардлагуудтай орчнууд энэхүү профайл дээр байгуулах эсвэл үүнийг солих боломжтой.

3.2. Гэрчилгээний шатлал ба итгэл

Нийтийн түлхүүрийн мэдлэг шаарддаг аюулгүй байдлын үйлчилгээний хэрэглэгч шаардлагатай нийтийн түлхүүрийг агуулж байгаа гэрчилгээг ерөнхийд нь олж авах болон батлах хэрэгтэй. Хэрвээ ГОБ-ийн нийтийн түлхүүрийн баталгаатай хуулбар, ГОБ-ийн нэр, хамааралтай мэдээлэл (жишээ гь хүчинтэй байх хугацаа эсвэл нэрийн хязгаарлалт)- ийг нийтийн түлхүүрийн хэрэглэгч аль хэдийн хадгалаагүй бол дараа нь нийтийн түлхүүр олж авахад нэмэлт гэрчилгээ хэрэгтэй болж магадгүй. Ерөнхийдөө, нэг ГОБ-ээр гарын үсэг зурагдсан нийтийн түлхүүрийн эзэмшигч (төгсгөлийн зүйл)-ийн гэрчилгээ, бусад ГОБ-уудаар гарын үсэг зурагдсан ГОБ-уудын тэг эсвэл түүнээс дээш нэмэлт гэрчилгээнүүд агуулсан гэрчилгээний гинжин хэлхээ шаардлагатай байж болно. Гэрчилгээний шатлал гэж нэрлэгддэг ийм гинжин хэлхээ шаардлагатай. Учир нь зөвхөн нийтийн түлхүүрийн хэрэглэгч хязгаарлагдмал тоогоор баталгаатай ГОБ-ийн нийтийн түлхүүрүүдийн хязгаарлагдмал тоотой эхэлсэн/загварчилсан/ байна.

Нийтийн түлхүүрийн хэрэглэгчид гэрчилгээний шатлалыг олж авах боломжтойгоор ГОБ-ууд Тохируулах боломжтой янз бүрийн арга замууд байдаг. ИНСШ-д зориулан RFC 1422 нь ГОБ-ын хатуу шаталсан бүтцийг тодорхойлсон. Энд гурван төрлийн ИНСШ гэрчилгээ олгогч байгуулга байна:

a) Интернэтийн Бодлогын Бүртгэлийн Байгуулга (ИББББ):Энэхүү байгуулга нь Интернэт Нийгмийн ивээлд үйл ажиллагаа явуулж ИНСШ гэрчилгээний шатлалын 1-р түшингийн үндсэн үйлдлийг хийдэг. Мөн зөвхөн БГБ-ууд буюу байгууллагуудын дараагийн түвшинд зориулсан гэрчилгээг олгох юм. Бүх гэрчилгээний шатлалууд ИББББ-аас эхэлнэ.

b) Бодлогын Гэрчилгээний Байгуулга (БГБ)-ууд нь шатлалын 2-р түвшинд байх ба ИББББ-аас нэг бүрчлэн баталгаажуулдаг. БГБ нь Баталгаажуулж байгаа Хэрэглэгч эсвэл Дэд эрх мэдэл бүхий гэрчилгээ олгогч байгууллагатай холбоотой түүний бодлогын мэдэгдлийг тогтоох болон хэвлэх ёстой. Ялгаатай БГБ-ууд ялгаатай хэрэглэгчийн хэрэгцээ шаардлагуудыг хангах зорилготой байна. Жишээ нь нэг БГБ (зохион байгуулалтын БГБ) арилжааны байгууллагуудын хэрэгцээнд ерөнхий цахим шуудан дэмжих боломжтой бол өөр нэг БГБ (өндөр баталгаатай БГБ) магадгүй тоон гарын үсгийн шаардлагуудыг хуульд нийцүүлэн

холбосон илүү хатуу бодлого/дүрэм боловсруулсан байж болно.

c) ГОБ-ууд бол шатлалын 3-р түвшний ба мөн доод түвшнүүдэд ажиллаж чадна. Тэдгээрийг 3-р түвшинд БГБ-уудаар баталгаажуулдаг. ГОБ-ууд жишээ нь тодорхой байгууллагууд, тодорхой байгууллагын нэгжүүд (тэнхимүүд, бүлгүүд, хэсгүүд гэх мэт) эсвэл тодорхой газарзүйн бүс нутгийг төлөөлдөг.

RFC 1422 цаашлаад нэрд захирагдахыг шаардах дүрэмтэй. Энэхүү дүрэмд зөвхөн ГОБ өөрийнхөө нэр (X.500 нэрийн модон дахь)-д захирагдах нэрсээр нэгжүүдэд зориулан гэрчилгээ олгоно. ИНСШ гэрчилгээний шатлалтай холбоотой итгэл/итгэлцэл нь БГБ нэр гэсэн утгатай. Нэрийг захирах дүрэм нь ГОБ-аас доош БГБ нь тэдний баталгаажуулж чадах (байгууллагад зориулсан ГОБ нь зөвхөн байгууллагын нэрийн модонд дахь нэгжүүдийг баталгаажуулна) харьяа байгууллагуудын багцаар ухаалгаар/мэдрэмжтэйгээр хязгаарлагдахыг баталгаажуулдаг. Гэрчилгээний хэрэглэгчийн системүүд дараах нэрийн захирах дүрмийг механикаар шалгаж боломжтой.

RFC 1422 нь X.509 хувилбар 1 гэрчилгээний форматыг ашигладаг. X.509 хувилбар 1-ийн хязгаарлалт нь хамааралтай бодлого/дүрмийн мэдээлэл эсвэл гэрчилгээний хэрэгслийг хязгаарлахыг тодорхойлох хэд хэдэн бүтцийн хязгаарлалт тавихыг шаарддаг. Тэдгээр хязгаарлалтууд багтаана:

a) ИББББ-аас эхлэлтэй бүх гэрчилгээний шатлалууд цэвэр дээрээс-доош шаталсан бүтэцтэй

b) ГОБ-ийн субъектүүдийн нэрсийг нэрийн захирах дүрэм хязгаарлана

c) БГБ-ийн үзэл баримтлалыг хэрэглэх нь гэрчилгээний гинжин гэрчилгээний логикт оруулсан бие даасан БГБ-уудын мэдлэгийг шаардана. Хэрвээ гинжийг зөвшөөрөх боломжтой бол бие даасан БГБ-уудын мэдлэгийг тодорхойлсон байх шаардлагатай.

X.509 хувилбар 3-тай хамт RFC 1422-д заасан ихэнх шаардлагуудыг ашигласан ГОБ-ийн бүтцийг хязгаарлах шаардлагагүйгээр гэрчилгээний өргөтгөл ашиглан шийдвэрлэх боломжтой. Тухайлбал, гэрчилгээний өргөтгөлүүдийг гэрчилгээний дүрмүүдтэй холбоотой БГБ-уудын хэрэгцээг арилгахын тулд ба хязгаарлалтын өргөтгөлүүдийг нэрийн захирагдах дүрмийн хэрэгцээг арилгахын тулд юм. Үр дүнд нь энэхүү баримт бичиг нь дараахыг агуулж илүү уян хатан архитектурыг дэмждэг:

a) гэрчилгээний шатлалууд хэрэглэгчийн өөрийн домэйн дахь ГОБ-ийн нийтийн түлхүүртэй хамт эсвэл шатлалын хамгийн дээд талын нийтийн

түлхүүрийн хамт эхэлнэ. Хэрэглэгчийн өөрийн домэйн дахь ГОБ-ийн нийтийн түлхүүртэйгээр эхлэх нь тодорхой давуу талуудтай. Зарим орчинд дотоод домэйн нь хамгийн итгэлтэй/найдвартай.

b) Нэрийн хязгаарлалтыг Гэрчилгээ дэх нэрийн хязгаарлалтын өргөтгөлүүдэд тодорхой оруулах замаар тавьж болно. Харин зайлшгүй шаардлагатай биш.

c) Дүрмийн өргөтгөлүүд болон дүрмийн зураглалууд нь автоматжуулалтын илүү дээд зөвшөөрлүүдээр БГБ үзэл баримтлалыг солино. Хэрвээ гэрчилгээний шатлалууд нь БГБ-уудын тухайлсан мэдлэгийн оронд гэрчилгээний агуулга дээр үндэслэн хүлээн зөвшөөрөх боломжтой бол Апп тодорхойлж болно. Энэ нь гэрчилгээний шатлал боловсруулалтын автоматжуулалтыг зөвшөөрдөг.

Х.509 хувилбар 3 нь ИНСШ-дэх шаардлагатай үндсэн мэдээллээс бусдад найдахыг багасгах ГОБ эсвэл Төгсгөлийн зүйл гэсэн гэрчилгээний субъектийг таних өргөтгөлийг агуулдаг.

Энэхүү тодорхойлолт нь ГОБ гэрчилгээнүүд ба төгсгөлийн зүйлийн гэрчилгээнүүд гэсэн хоёр ангиллын гэрчилгээг хамарна. ГОБ гэрчилгээнүүдийг цааш хөндлөн-гэрчилгээнүүд (хялбарчилсан-гэрчилгээ), өөрөө гаргасан гэрчилгээнүүд, өөрөө гарын үсэг зурсан гэрчилгээнүүд гэж гурван ангилалд хуваагдана. Хөндлөн-гэрчилгээнүүд нь олгогч ба субъектүүд нь ялгаатай зүйл байдаг ГОБ гэрчилгээнүүд юм. Хөндлөн-гэрчилгээнүүдээр хоёр ГОБ-уудын хоорондын харилцааны итгэлцлийг тодорхойлно. Өөрөө гаргасан гэрчилгээнүүд нь олгогч ба субъектүүд нь ижил зүйл байдаг ГОБ гэрчилгээнүүд юм. Өөрөө гаргасан гэрчилгээнүүдийг дүрэм эсвэл үйл ажиллагааны өөрчлөлтийг дэмжихээр үүсгэдэг. Өөрөө гарын үсэг зурсан гэрчилгээнүүд гэж тоон гарын үсгийг гэрчилгээ дотор байршсан нийтийн түлхүүрээр баталгаажуулж болдог өөрөө гаргасан гэрчилгээнүүд юм. Өөрөө гарын үсэг зурсан гэрчилгээнүүдийг гэрчилгээний шатлалыг эхлүүлэхэд хэрэглэх зорилгоор нийтийн түлхүүрийг зөөх/тээвэрлэхэд ашигладаг. Төгсгөлийн зүйлийн гэрчилгээнүүдийг гэрчилгээ олгох/гаргах эрхгүй субъектэд олгогддог.

3.3. Хүчингүй болгох

Гэрчилгээ олгогдохдоо түүнийг бүхэлд нь хүчинтэй байх хугацаанд ашиглагдахаар төлөвтэй байна. Хэдий тийм боловч хүчинтэй байх хугацаа дуусахаас өмнө янз бүрийн нөхцөл байдал үүсгэж гэрчилгээ хүчингүй болж болно. Ийм нөхцөл нь нэрээ солих, ГОБ ба субъектийн хоорондын холбоог өөрчлөх (жишээ нь ажилтан байгууллагатай хөдөлмөрийн гэрээг дуусгавар

болгох), харгалзах хувийн түлхүүрийн тохиролцоо эсвэл сэжигтэй тохиролцоо зэрэг орно. Ийм нөхцөл байдал үүсвэл ГОБ нь гэрчилгээг хүчингүй болгох шаардлагатай.

Х.509-д гэрчилгээг хүчингүй болгох нэг аргыг тодорхойлдог. Энэхүү аргыг ХГЖ гэж нэрлэх ба ГОБ бүр гарын үсэг зурсан өгөгдлийн бүтцийг давтамжтайгаар хэвлэн гаргах орно. ХГЖ бол ГОБ эсвэл ХГЖ олгогчоор гарын үсэг зурагдсан болон нийтийн мэдээллийн санд чөлөөтэй ашиглах боломжтойгоор байршуулсан хүчингүй болгосон гэрчилгээнүүдийг таних time-stamped жагсаалт юм. Хүчингүй болгосон гэрчилгээ бүрийг ХГЖ дэх түүний серийн дугаараар таньдаг. Гэрчилгээ ашигладаг систем нь гэрчилгээг хэрэглэх (жишээ нь алсын хэрэглэгчийн тоон гарын үсгийг баталгаажуулах) үед систем зөвхөн гэрчилгээний гарын үсэг болон хүчинтэй байдлыг шалгахгүй. Харин тохиромжтой сүүлийн ХГЖ-ийг олж авч гэрчилгээний серийн дугаараар тэрхүү ХГЖ-д байхгүй эсэхийг шалгана. Тохиромжтой сүүлийн гэсэн утга нь дотоод журамтай холбоотойгоор ялгаатай байж болох ч ихэнхдээ хамгийн сүүлд гарсан ХГЖ гэсэн утгыг илэрхийлнэ. Шинэ ХГЖ тогтмол хугацааны давтамжтай хэвлэгддэг (жишээ нь цаг тутамд, өдөрт, эсвэл долоо хоногт). ХГЖ-д бүртгэл нэмэгдсэн гэдэг нь дараагийн шинэчлэлтийн нэг хэсэгтэй адил хүчингүй болгох тухай мэдэгдэл юм. Хүчингүй болгосон гэрчилгээний хүчинтэй хугацаа тогтмол хуваарьт хэвлэгддэг ХГЖ-д гарч ирэх хүртэл бүртгэлийг ХГЖ-ээс хасаж БОЛОХГҮЙ.

Энэхүү хүчингүй болгох аргын давуу тал нь гэрчилгээнүүдтэй өөрсөдтэйн яг ижил утгаар тухайлбал найдваргүй серверүүд болон найдваргүй холболтуудаар магадгүй тараасан ХГЖ байж болно.

Найдваргүй холболт болон серверүүдийг ашиглаж байхад ХГЖ хүчингүй болгох аргын нэг хязгаарлалт нь ХГЖ гарах хугацаагаар хязгаарлагддаг хүчингүй болгох хугацаа хоорондын зай юм. Жишээ нь хэрвээ хүчингүй болгохыг сая мэдээлсэн бол хүчингүй болгох тухай нь хэвлэгдсэн байгаа ХГЖ-уудын төлөвлөгөөт шинэчлэл хийгдэх хүртэл гэрчилгээ-хэрэглэгч системүүдэд найдвартай мэдэгдэх боломжгүй. Энэ нь ХГЖ хэвлэгддэг давтамжаас хамааран магадгүй нэг цаг, нэг өдөр, нэг долоо хоногт шинэчлэгдэж болно.

Х.509 хувилбар 3 гэрчилгээний форматын нэгэн адил олон үйлдвэрлэгчээс харилцан ажиллах боломжтойгоор хэрэгжүүлэлтийг хөнгөвчлөхийн тулд Х.509 хувилбар 2 ХГЖ форматыг интернэтэд ашиглахад зориулан профайл хийх шаардлагатай. Энэ профайлыг тодорхойлох нь энэ баримт бичгийн нэг зорилго юм. Гэхдээ энэ профайл нь ХГЖ гаргах шаардлагагүй. Онлайнаар хүчингүй

болгох мэдэгдлийг дэмждэг мессежний формат, протоколуудыг бусад НТДБХ техникийн үзүүлэлтүүдэд тодорхойлсон. Зарим орчинд X.509 ХГЖ-ийн өөр хувилбар болгон хүчингүй болгох мэдэгдлийн онлайн аргыг хэрэглэж болно. Хүчингүй болсныг онлайнаар шалгах нь хүчингүй болсон тухай тайлан болон холбогдох талуудад мэдээлэл түгээх хоцролтыг мэдэгдэхүйц бууруулж чадна. Зөвхөн ГОБ нь хүчингүй болгох тайланг жинхэнэ бөгөөд хүчинтэй гэж хүлээн зөвшөөрсний дараа онлайн үйлчилгээнд өгөх аливаа асуулга нь хүчингүй болгосны гэрчилгээ баталгаажуулалтын нөлөөг зөв тусгах болно. Гэсэн хэдий ч эдгээр аргууд нь аюулгүй байдлын шинэ шаардлагуудыг тавьдаг: гэрчилгээ баталгаажуулагч нь онлайн баталгаажуулалтын үйлчилгээнд итгэх шаардлагатай бөгөөд хадгалах газарт итгэх шаардлагагүй.

3.4. Үйл ажиллагааны протоколууд

Үйл ажиллагааны протоколууд нь гэрчилгээнүүд болон ХГЖ-уудыг (эсвэл төлөвийн мэдээлэл) гэрчилгээг ашиглаж байгаа хэрэглэгчийн системүүдэд хүргэхэд шаардлагатай. LDAP, HTTP, FTP, X.500 дээр суурилсан түгээх үйл ажиллагааг багтаах гэрчилгээ болон ХГЖ хүргэлтийн өөр өөр арга хэрэгслийн олон төрөлд зориулсан заалтууд хэрэгтэй байна. Үйл ажиллагааны протоколууд нь бусад НТДБХ тодорхойлолтуудад тодорхойлогдсон тэдгээр функцүүдийг дэмждэг байна. Эдгээр тодорхойлолтууд Мессежний формат, дээр дурдсан үйл ажиллагааны орчнууд бүгдийг дэмжихэд зориулсан боловсруулалт, хамааралтай MIME контентын төрлүүдийн эшлэх эсвэл агуулж байгаа тодорхойлолтуудыг багтааж болно.

3.5. Удирдлагын протоколууд

Удирдлагын протоколууд нь НТДБ-ийн хэрэглэгч болон удирдлагын нэгжийн хоорондын онлайн харилцан үйлчлэлийг дэмжихийг шаарддаг. Жишээ нь удирдлагын протоколыг түлхүүрийн хослолоор холбогдсон ГОБ ба түүний хэрэглэгчийн систем хооронд, эсвэл ГОБ-ууд хооронд хийх хөндлөн баталгаажуулахад ашиглаж болно. Удирдлагын протоколоор дэмжигдэх шаардлагатай байж болзошгүй Функцүүдийн багцад дараах зүйлс багтана:

a) бүртгэл: Энэ нь тухайн ГОБ нь тухайн хэрэглэгчдийг гэрчлэх, эсвэл гэрчилгээ олгохоос өмнө хэрэглэгч өөрийгөө ГОБ-д (шууд эсвэл ББ-аар дамжуулан) таниулах үйл явц юм.

b) эхлүүлэх: Хэрэглэгчийн систем аюулгүй ажиллахын өмнө, дэд бүтцийн хувьд өөр газар хадгалагдсан түлхүүрүүдтэй тохирох гол түлхүүрийн материалыг суурилуулах шаардлагатай. Жишээлбэл, гэрчилгээний шатлалыг шалгахад ашиглахын тулд хэрэглэгчийн итгэмжлэгдсэн

ГОБ(ууд)-ын нийтийн түлхүүр болон бусад баталгаатай мэдээллээр аюулгүй эхлүүлэх шаардлагатай.

Цаашилбал, хэрэглэгч ихэвчлэн өөрийн түлхүүрийн хослолуудтай эхлүүлэх шаардлагатай.

c) баталгаажуулалт: Энэ нь ГОБ хэрэглэгчийн нийтийн түлхүүрийн гэрчилгээг олгож, тухайн гэрчилгээг хэрэглэгчийн клиент системд буцааж өгөх ба/эсвэл уг гэрчилгээг хадгалах газарт байршуулах үйл явц юм.

d) түлхүүрийн хослолыг сэргээх: Сонголтын хувьд хэрэглэгчийн клиент түлхүүрийн материалыг (жишээ нь, шифрлэлтийн зорилгоор ашигладаг хэрэглэгчийн хувийн түлхүүр) ГОБ эсвэл түлхүүр нөөцлөх системээр нөөцөлж болно. Хэрэв хэрэглэгч эдгээр нөөцлөгдсөн түлхүүрийн материалыг сэргээх шаардлагатай бол (жишээлбэл, мартагдсан нууц үг эсвэл алдагдсан түлхүүрийн гинжний файлын үр дүнд) сэргээх ажиллагааг дэмжихийн тулд онлайн протоколоор солилцох хэрэгтэй байж магадгүй юм.

e) түлхүүрийн хослолыг шинэчлэх: Бүх түлхүүрийн хосыг тогтмол шинэчилж байх шаардлагатай, өөрөөр хэлбэл шинэ түлхүүрээр сольж, шинэ гэрчилгээ олгох шаардлагатай.

f) хүчингүй болгох хүсэлт: Эрх бүхий хүн гэрчилгээг хүчингүй болгох шаардлагатай хэвийн бус нөхцөл байдлын талаар ГОБ-д зөвлөнө/мэдэгдэнэ.

g) хөндлөн-баталгаажуулалт: Хоёр ГОБ нь хөндлөн гэрчилгээг бий болгоход ашигласан мэдээллээ солилцдог. Хөндлөн гэрчилгээ гэдэг нь нэг ГОБ-аас нөгөө ГОБ-д олгосон, олгож байгаа гэрчилгээнд зориулсан ГОБ гарын үсгийн түлхүүрийг агуулсан гэрчилгээ юм.

Онлайн протоколууд нь дээрх функцүүдийг хэрэгжүүлэх цорын ганц арга зам биш гэдгийг анхаарна уу. Бүх функцийн хувьд ижил үр дүнд хүрэх офлайн аргууд байдаг бөгөөд энэ тодорхойлолт нь онлайн протокол ашиглахыг шаарддаггүй. Жишээлбэл, техник хангамжийн жетоныг ашиглах үед олон функцийг биет жетон хүргэх хэсэг болгон гүйцэтгэж болно. Цаашилбал, дээрх функцүүдийн заримыг нэг протокол солилцоонд нэгтгэж болно. Ялангуяа бүртгэл, эхлүүлэх, баталгаажуулах хоёр ба түүнээс дээш функцийг нэг протокол солилцоонд нэгтгэж болно.

4. Гэрчилгээ ба гэрчилгээний өргөтгөлийн профайл

Энэ бүлэгт харилцан ажиллах чадвар болон дахин хэрэглэх НТДБ-г дэмжих Нийтийн түлхүүрийн гэрчилгээнүүдэд зориулсан профайлыг танилцуулна. Энэ бүлэг нь X.509 хувилбар 3 гэрчилгээний формат болон x.509-д тодорхойлсон стандарт гэрчилгээний өргөтгөлүүд дээр суурилна. ISO/IEC, ITU-T- ийн баримт бичгүүд ASN.1-ийн 1997 оны хувилбарыг хэрэглэдэг: мөн 1988 ASN.1 өгүүлбэрзүйг энэ баримт бичигт хэрэглэх шифрлэгдсэн гэрчилгээ болон стандарт өргөтгөлүүд ижил тэнцүү. Энэ бүлэгт мөн Интернэтийн нийгэмлэгүүдэд зориулсан НТДБ-г дэмжихэд шаардлагатай хувийн өргөтгөлүүдийг тодорхойлно.

Гэрчилгээг өргөн хүрээний хамтын ажиллагааны зорилго, үйл ажиллагааны болон баталгааны шаардлагуудын өргөн хүрээг хамарсан өргөн хүрээний хэрэглээ, орчинд ашиглаж болно. Энэхүү баримт бичгийн зорилго нь өргөн хүрээний харилцан үйлчлэл, хязгаарлагдмал тусгай зориулалтын шаардлагуудыг шаарддаг ерөнхий хэрэглээний нийтлэг үндэслэлийг бий болгох явдал юм. Ялангуяа албан бус интернэт цахим шуудан, IPsec, WWW программуудад X.509 хувилбар 3 гэрчилгээ ашиглахыг дэмжихэд онцгойлон анхаарах болно.

4.1. Үндсэн гэрчилгээний талбарууд

X.509 хувилбар 3 гэрчилгээний үндсэн өгүүлбэрзүй нь дараахтай адил юм. Гарын үсгийн тооцоололд зориулан гарын үсэг зурах өгөгдөл нь ASN.1 онцолсон шифрлэх дүрмүүд (DER) [X.690]- ийг ашиглаж шифрлэгдсэн байна. ASN.1 DER шифрлэлт бол элемент бүрд зориулсан шошго, урт, утгыг шифрлэж байгаа систем юм.

```
Certificate  ::=  SEQUENCE  {
    tbsCertificate       TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
    version         [0]  EXPLICIT  Version DEFAULT v1,
    serialNumber         CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
```

```
    issuerUniqueID  [1]  IMPLICIT  UniqueIdentifier OPTIONAL,
                         - - If present, version MUST be v2 or v3
    subjectUniqueID [2]  IMPLICIT  UniqueIdentifier OPTIONAL,
                         - - If present, version MUST be v2 or v3
    extensions      [3]  EXPLICIT  Extensions OPTIONAL
                         - - If present, version MUST be v3
    }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time }

Time ::= CHOICE  {
    utcTime        UTCTime,
    generalTime    GeneralizedTime  }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
    algorithm            AlgorithmIdentifier,
    subjectPublicKey     BIT STRING   }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET  STRING
                - - contains the DER encoding of an ASN.1 value
                - - corresponding to the extension type identified
                - - by extnID
    }
```

Дараах зүйлс нь X.509 хувилбар 3 гэрчилгээг Интернэтэд хэрэглэхэд зориулан тодорхойлно.

4.1.1. Гэрчилгээний талбарууд

Гэрчилгээ бол гурван шаардлагатай талбаруудын дараалал юм. Талбаруудыг дараах дэд бүлгүүдэд нарийвчлан тайлбарласан.

4.1.1.1. tbsCertificate

Энэ талбар нь Субъект ба олгогчийн нэр, субъекттэй холбоотой нийтийн түлхүүр, хүчинтэй байх хугацаа, бусад холбоотой мэдээллийг агуулна. Талбарууд нь 4.1.2-д нарийвчлан тайлбарласан. tbsCertificate нь 4.2-д тодорхойлогдсон өргөтгөлүүдийг ихэвчлэн агуулна.

4.1.1.2. signatureAlgorithm

signatureAlgorithm талбар нь ГОБ-аар гэрчилгээнд гарын үсэг зурахад ашиглагдсан крифтографикийн алгоритмын адилтгагчийг агуулна. [RFC3279], [RFC4055], [RFC4491] жагсаалт гарын үсгийн алгоритмуудыг дэмждэг, мөн бусад гарын үсгийн алгоритмуудыг дэмждэг БАЙЖ БОЛНО.

Алгоритмын адилтгагч нь дараах ASN.1 бүтцээр тодорхойлогдоно:

```
AlgorithmIdentifier ::= SEQUENCE  {
    algorithm             OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL  }
```

Алгоритмын танигч нь крифтографийн алгоритмыг ялган танихад хэрэглэгддэг. OBJECT IDENTIFIER бүрэлдэхүүн нь алгоритм (жишээ нь SHA-1- тай DSA)-ыг тодорхойлдог. Заавал биш параметрүүдийн талбарын агуулга нь тодорхойлсон алгоритмуудаас хамааран өөр өөр байх болно.

Энэ талбар нь дараал tbsCertificate (4.1.2.3) дахь гарын үсэг талбартай адил алгоритм адилтгагчийг ЗААВАЛ агуулах ёстой.

4.1.1.3. signatureValue

signatureValue талбар нь the ASN.1 DER encoded tbsCertificate шифрлэгдсэн дээр тооцоологдсон Тоон гарын үсгийг агуулна. ASN.1 DER encoded tbsCertificate нь гарын үсгийн функцийн оролт шиг ашиглагдана. Гарын үсгийн утга бол BIT STRING шиг ба гарын үсгийн талбарт агуулагдана. Энэ үйлдлийн нарийвчилсан мэдээллийг [RFC3279], [RFC4055], [RFC4491]- д жагсаасан алгоритм бүрийн хувьд зааж өгсөн болно.

Энэ Гарын үсгийг үүсгэснээр, ГОБ нь tbsCertificate талбар дахь мэдээллийн хүчинтэй байдлыг баталгаажуулна. Тухайлбал ГОБ нь нийтийн түлхүүрийн материал болон гэрчилгээний субъект хоорондох холболтыг баталгаажуулдаг.

4.1.2. TBSCertificate

Дараалах TBSCertificate нь гэрчилгээний субъект болон гэрчилгээг олгосон ГОБ-тай холбоотой мэдээллийг агуулна. TBSCertificate бүр субъект болон олгогчийн нэр, субъекттэй холбоотой нийтийн түлхүүр, хүчинтэй хугацаа, хувилбарын дугаар, серийн дугаар агуулна. Эдгээрийн зарим нь заавал биш

өвөрмөц адилтгагч талбаруудыг агуулдаг БАЙЖ БОЛНО. Энэ бүлгийн үлдсэн хэсэгт эдгээр талбаруудын өгүүлбэрзүй болон утгазүйг тодорхойлно. TBSCertificate өргөтгөл нь ихэвчлэн өргөтгөлүүдийг агуулна. Бүлэг 4.2-д Интернэт НТДБ-д зориулсан өргөтгөлүүдийг тодорхойлсон.

4.1.2.1. Хувилбар

Энэ талбар нь шифрлэгдсэн гэрчилгээний хувилбарын тодорхойлно. Өргөтгөлүүдийг хэрэглэсэн үед болон энэ профайлд найдвал хувилбар нь 3 (утга нь 2) ЗААВАЛ байх ёстой. Хэрвээ ямар нэгэн өргөтгөл байхгүй бөгөөд UniqueIdentifier-ийг байгаа бол хувилбар нь 2 (утга нь 1) байх ХЭРЭГТЭЙ; гэсэн хэдий ч хувилбар нь 3 БАЙЖ БОЛНО. Хэрвээ зөвхөн үндсэн талбарууд байвал хувилбар нь 1 (утга нь дефаулт утга шиг гэрчилгээнээс орхигдуулна) байх ХЭРЭГТЭЙ; Гэсэн хэдий ч хувилбар нь 2 эсвэл 3 БАЙЖ БОЛНО.

Хэрэгжүүлэлт нь гэрчилгээний дурын хувилбарыг зөвшөөрөхөөр бэлдсэн байх ХЭРЭГТЭЙ. Хамгийн багадаа нийцлийн хэрэгжүүлэлт нь хувилбар 3 гэрчилгээг ЗААВАЛ хүлээн зөвшөөрөхөөр байх ёстой.

Энэ профайл дээр суурилсан хэрэгжүүлэлт нь Хувилбар 2 гэрчилгээний үе үүснэ гэж найдаагүй.

4.1.2.2. Серийн дугаар

Серийн дугаар нь гэрчилгээ бүрд ГОБ-аар олгогдсон Эерэг бүхэл тоон утга ЗААВАЛ байна. Энэ нь гэрчилгээ бүрийг өгсөн ГОБ (олгогчийн нэр болон серийн дугаараар давтагдашгүй гэрчилгээг адилтгах гэх мэт)-ээр олгосон давтагдашгүй ЗААВАЛ байна. ГОБ-ууд сөрөг-биш бүхэл тоон утгыг serialNumber-т force байх ёстой.

4.1.2.3. Гарын үсэг

Энэ талбар гэрчилгээнд гарын үсэг зурахад ГОБ-ийн ашигладаг алгоритмын адилтгагчийг агуулагдана.

Энэ талбар нь Дараалах гэрчилгээ (4.1.1.2) дэх signatureAlgorithm талбартай адил алгоритмын адилтгагчийг ЗААВАЛ агуулна. Заавал биш параметрүүдийн талбарын агуулга нь тодорхойлсон алгоритмын дагуу өөр өөр байх болно. [RFC3279], [RFC4055], [RFC4491] жагсаалт гарын үсгийн алгоритмуудыг дэмжигдэг боловч бусад гарын үсэг зурах алгоритмуудыг бас дэмждэг БАЙЖ БОЛНО.

4.1.2.4. Олгогч

Олгогчийн талбар нь гэрчилгээ олгосон болон гарын үсэг зурсан нэгжийг

тодорхойлно. Олгогчийн талбар хоосон бус ялгагдах нэр (ЯН)-ийг ЗААВАЛ агуулна. Олгогчийн талбарыг X.501 төрлийн Нэр [X.501] гэж тодорхойлсон. Нэрийг дараах ASN.1 бүтцээр тодорхойлно.

```
Name ::= CHOICE  {- - only one possibility for now- -
  rdnSequence  RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::=
  SET SIZE (1..MAX) OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
  type     AttributeType,
  value    AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY- - DEFINED BY AttributeType

DirectoryString ::= CHOICE  {
      teletexString           TeletexString  (SIZE (1..MAX)),
      printableString         PrintableString (SIZE (1..MAX)),
      universalString         UniversalString (SIZE (1..MAX)),
      utf8String              UTF8String  (SIZE (1..MAX)),
      bmpString               BMPString (SIZE (1..MAX)) }
```

Нэр нь улсын нэр гэх мэт атрибутууд болон АНУ зэрэг харгалзах утгуудаас бүрдсэн шаталсан нэрийг тодорхойлдог. AttributeValue бүрэлдэхүүн хэсгийн төрлийг AttributeType-ээр тодорхойлно; ерөнхийдөө энэ нь DirectoryString байх болно.

DirectoryString төрөл нь PrintableString, TeletexString, BMPString, UTF8String, болон UniversalString гэсэн сонголтоор тодорхойлогддог. Энэ профайлтай таарч байгаа ГОБ-ууд нь хоёр үл хамаарах зүйлээс бусад тохиолдолд DirectoryString-ийн PrintableString эсвэл UTF8String шифрлэлтийг ЗААВАЛ ашиглах ёстой. ГОБ-ууд өмнө нь TeletexString, BMPString, эсвэл UniversalString ашиглан шифрлэгдсэн атрибутууд бүхий гаргагчийн талбар бүхий гэрчилгээ олгосон бол ГОБ нь хоцрогдсон нийцтэй байдлыг хадгалахын тулд DirectoryString шифрлэлтүүдийг үргэлжлүүлэн ашигладаг БАЙЖ БОЛНО. Түүнчлэн, одоо байгаа ГОБ-ууд TeletexString, BMPString, эсвэл UniversalString ашиглан шифрлэгдсэн атрибутууд бүхий гаргагчийн талбар бүхий гэрчилгээ

олгодог домэйнд нэмэгдсэн шинэ ГОБ-ууд нь одоо байгаа ГОБ-уудтай ижил шифрлэлтүүдийг ашиглан одоо байгаа ГОБ-уудтай хуваалцаж буй атрибутуудыг шифрлэдэг БАЙЖ БОЛНО.

Дээр дурдсанчлан ялгагдах нэрс нь атрибутуудаас бүрддэг. Энэ тодорхойлолт нь нэрд гарч болох атрибутын багцыг хязгаарладаггүй. Гэсэн хэдий ч, нийцсэн хэрэгжүүлэлтүүд нь доор тодорхойлсон атрибутын багцыг агуулсан гаргагчийн нэр бүхий гэрчилгээг хүлээн авахад бэлтгэх ёстой. Энэхүү тодорхойлолт нь нэмэлт атрибутын төрлүүдэд дэмжлэг үзүүлэхийг ЗӨВЛӨЖ БАЙНА.

атрибутуудын Стандартын багцуудыг тодорхойлолтууд [X.520]-ийн X.500 цувралд тодорхойлсон. Энэхүү тодорхойлолтын хэрэгжилт нь олгогч болон субъектийн (4.1.2.6) нэрэн дэх дараах стандарт атрибутын төрлүүдийг хүлээн авахад бэлтгэгдсэн байх ёстой.

- Улс
- Байгууллага
- Байгууллагын нэгж
- Ялгагдах нэрийн шалгуур үзүүлэлт
- Хот эсвэл бүсийн нэр
- Нийтлэг нэр
- Серийн дугаар

Нэмээд энэ тодорхойлолтын хэрэгжүүлэлтэд олгогч болон субъектийн нэрсэнд дараах стандарт атрибутын төрлүүдийг хүлээн авахаар бэлдсэн байх ХЭРЭГТЭЙ.

- нутаг дэвсгэр,
- гарчиг,
- овог,
- өөрийн нэр,
- эхний үсэг,
- нууц нэр, ба
- үеийн шалгуур үзүүлэлт (жишээ нь, "Jr.", "3rd", эсвэл "IV").

Өгүүлбэрзүй болон Эдгээр атрибутын төрлүүдэд холбоотой объектын адилтгагч Хавсралт А дахь ASN.1 модулиудад тусгагдсан.

Нэмж дурдахад, [RFC4519]-д тодорхойлсонтой адилаар энэ тодорхойлолтыг хэрэгжүүлэхдээ domainComponent атрибутыг хүлээн авахаар ЗААВАЛ бэлтгэсэн байна. Домэйн Нэрийн Систем (DNS) нь шаталсан нөөцийн шошгожуулах системийг хангана. Энэ атрибут нь DNS нэрсээр зэрэгцүүлэх DNS-ийг хэрэглэх байгууллагад зориулсан тохиромжтой механизмаар хангана.

Энэ нь нэрийн нэмэлт өргөтгөлүүдийн dNSName бүрэлдэхүүн хэсгүүдэд зориулсан орлуулах зүйл биш юм. Хэрэгжүүлэлтэд нэрсийг DNS нэр болгон хөрвүүлэх шаардахгүй. Энэ атрибутын төрөлд зориулсан өгүүлбэрзүй болон холбогдох ОА-ийг Хавсралт А дахь ASN.1 модулиудад зааж өгсөн болно. domainComponent атрибутын төрөлтэй хамт ашиглахад зориулан шифрлэлд олон улсын домэйн нэрийн дүрмийг бүлэг 7.3-д заасан.

Олгогчийн Онцлог нэр болон субъектийн Онцлог нэр (4.1.2.6) талбарууд гэрчилгээний шатлалын шалгахад зориулан нэрийн гинжийг хийж Гэрчилгээний хэрэглэгчид боловсруулахад ЗААВАЛ бэлтгэсэн байна. Нэрийн гинж нь ГОБ гэрчилгээ дэх субъектийн нэртэй хамт нэг гэрчилгээ дэх олгогчийн Онцлог нэрийг тулгах байдлаар гүйцэтгэдэг. Онцлог нэрсийг харьцуулах дүрмийг 7.1-д заасан болно. Хэрвээ гэрчилгээ дэх олгогч болон субъект талбаруудад байх нэрсийг 7.1-д заасан дүрмийн дагуу тулгах бол гэрчилгээ нь өөрөө-өгсөн байна.

4.1.2.5. Хүчин төгөлдөр байх

Гэрчилгээний хүчинтэй байх хугацаа нь гэрчилгээний төлөвийн талаарх мэдээллийг ГОБ баталгаажуулж байх хугацаа юм. Энэ талбар нь гэрчилгээний хүчинтэй хугацааны эхэлсэн огноо (Өмнө биш) ба гэрчилгээний хүчинтэй байх хугацааны дуусах огноо (Дараа нь биш) гэсэн хоёр огнооны дараалал хэлбэрээр илэрхийлэгдэнэ. notBefore болон notAfter хоёулаа UTCTime эсвэл GeneralizedTime гэж шифрлэгдсэн байж болно.

Энэ профайлтай нийцүүлэн ГОБ нь UTCTime- тай адил 2049 он хүртэл гэрчилгээний хүчинтэй байх огноонуудыг ЗААВАЛ шифрлэнэ. Мөн GeneralizedTime- тай адилаар 2050 ба түүнээс хойших огноонуудыг ЗААВАЛ шифрлэнэ. Программууд нь UTCTime эсвэл GeneralizedTime-ийн Тохиромжтойгоор шифрлэгдсэн хүчинтэй байх хугацааг ЗААВАЛ боловсруулна.

Гэрчилгээний хүчинтэй байх хугацаа нь notBefore-аас notAfter хүртэлх хугацааг багтаасан хугацаа юм.

Зарим тохиолдолд төхөөрөмжүүдэд хүчинтэй байх хугацаа нь тодорхойгүй гэрчилгээ өгдөг. Жишээлбэл, төхөөрөмжид түүний загвар, серийн дугаарыг нийтийн түлхүүртэй холбосон гэрчилгээ олгож болно; Ийм гэрчилгээ нь төхөөрөмжийн ашиглалтын туршид хэрэглэгдэх зориулалттай юм.

Заагч гэх гэрчилгээнд хүчинтэй байх хугацаа тодорхой байдаггүй, харин 99991231235959Z гэсэн GeneralizedTime- ийн утгыг notAfter- т оноосон байх ХЭРЭГТЭЙ.

Олгогч нь notAfter огноо хүртэл төлөвийн мэдээллийг хадгалах боломжгүй

болох үед (үүнд notAfter огноо нь 99991231235959Z байх багтана), төлөвийн мэдээллийг засварлах үйлчилгээ дуусгавар болсны дараа гэрчилгээнд зориулсан хүчинтэй гэрчилгээний баталгаажуулалтын шатлал байхгүй эсэхийг олгогч ЗААВАЛ баталгаажуулна. Энэ нь бүх ГОБ гэрчилгээний хугацаа дуусах эсвэл хүчингүй болгох замаар хэрэгжиж болно. Тэдгээр гэрчилгээнүүд нь гэрчилгээ дэх гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүрийг агуулж байгаа болон гэрчилгээ дэх гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүрийг итгэлцлийн зангуу болгон ашиглахыг зогсоох байгаа болно

4.1.2.5.1. UTCTime

Бүх нийтийн цагийн төрөл болох UTCTime нь огноо, цагийг дүрслэх зорилготой стандарт ASN.1 төрөл юм. UTCTime нь бага эрэмбийн хоёр цифрээр жилийг зааж өгөх ба цагийг нэг минут эсвэл нэг секундийн нарийвчлалтайгаар зааж өгдөг. UTCTime нь Z (Зулу, Гринвичийн дундаж цаг) эсвэл цагийн зөрүүг агуулдаг.

Энэхүү профайлын зорилгод зориулан UTCTime утгуудыг ЗААВАЛ Гринвичийн дундаж цагаар (Зулу) илэрхийлэх, секундийг тэг байсан ч ЗААВАЛ багтаана (жишээ нь, цагийг YYMMDDHHMMSSZ). Тохиромжтой системүүд жил талбарыг (YY) дараах байдлаар ЗААВАЛ тайлбарлах ёстой.

YY нь 50-тай тэнцүү эсвэл илүү байхад жил нь 19YY- тай адилаар тайлбарлах ЁСТОЙ. Мөн YY нь 50-аас бага байхад 20YY- тай адилаар тайлбарлах ЁСТОЙ

4.1.2.5.2. GeneralizedTime

Ерөнхий цагийн төрөл болох GeneralizedTime нь хугацааг хувьсах нарийвчлалтайгаар дүрслэх стандарт ASN.1 төрөл юм. Нэмэлтээр, GeneralizedTime талбар нь орон нутгийн болон Гринвичийн дундаж цагийн хоорондох цагийн зөрүүний дүрслэлийг агуулж болно.

Энэхүү профайлын зорилгод зориулан GeneralizedTime утгуудыг ЗААВАЛ Гринвичийн дундаж цагаар (Зулу) илэрхийлэх, секундийг тэг байсан ч ЗААВАЛ багтаана (жишээ нь, цаг нь YYYYMMDHHMMSSZ). GeneralizedTime утгууд бутархай секундийг багтааж БОЛОХГҮЙ

4.1.2.6. Субъект

Субъект талбар нь субъектийн нийтийн түлхүүрийн талбарт хадгалагдсан нийтийн түлхүүртэй холбоотой нэгжийг тодорхойлно. Субъектийн нэрийг субъект талбар болон/эсвэл SubjectAltName өргөтгөлд оруулж авч явдаг БАЙЖ БОЛНО. Хэрэв субъект нь ГОБ (жишээ нь, 4.2.1.9-д дурдсанчлан үндсэн хязгаарлалтуудын өргөтгөлд байгаа CA-ийн утга ҮНЭН гэж дүрслэгдсэн) бол,

тухайн субъект талбарыг Субъект ГОБ-аас олгосон бүх гэрчилгээнд олгогч талбарын (4.1.2.4) агуулгатай хоосон бус онцгой нэр тохирч байхаар ЗААВАЛ бөглөх ёстой. Хэрэв субъект нь ХГЖ олгогч (жишээ нь, 4.2.1.3-т дурдсанчлан түлхүүрийн хэрэглээний өргөтгөлд байгаа cRLSign-ийн утга ҮНЭН гэж дүрслэгдсэн) бол тухайн сэдвийн талбарыг дараахтай тохирох хоосон бус нэрээр бөглөх ёстой. Субъект ХГЖ олгогчийн гаргасан бүх ХГЖ- д олгогч талбар (5.1.2.3)-ын агуулгатай хоосон бус онцгой нэр тохирч байхаар ЗААВАЛ бөглөх ёстой. Хэрэв субъектийг нэрлэх мэдээлэл нь зөвхөн subjectAltName өргөтгөлд (жишээ нь, зөвхөн и-мэйл хаяг эсвэл URI-д түлхүүр уягдсан) байгаа бол субъектийн нэр нь ЗААВАЛ хоосон дараалал байх ёстой бөгөөд SubjectAltName өргөтгөл нь ЗААВАЛ чухал байна.

Хоосон биш үед субъект талбарт X.500 ялгах нэр (ЯН) ЗААВАЛ байх ёстой. ЯН нь олгогч талбарт тодорхойлогдсон нэг ГОБ-ээр баталгаажих субъектийн нэгж бүрд зориулан ЗААВАЛ давтагдашгүй байх ёстой. ГОБ нь ижил субъектийн нэгжид ижил ЯН- тай нэг болон түүнээс олон гэрчилгээ олгодог БАЙЖ БОЛНО.

Субъект талбар нь X.501 төрлийн нэртэй адил тодорхойлогддог. Энэ талбарыг хэрэгжүүлэхэд тавигдах шаардлагууд нь олгогч талбар (4.1.2.4)-т тодорхойлсон шаардлагууд юм. Энэхүү тодорхойлолтын хэрэгжилт нь олгогч талбарт зориулсан шаардлагатай атрибутуудын төрлүүдийг агуулж байгаа субъектийн нэрийг хүлээн авахад ЗААВАЛ бэлтгэгдсэн байна. Энэхүү тодорхойлолтын хэрэгжилт нь олгогч талбарт зориулсан санал болгосон атрибутуудын төрлүүдийг агуулж байгаа субъектийн нэрийг хүлээн авахад бэлтгэгдсэн байх ХЭРЭГТЭЙ. Эдгээр атрибутуудад зориулсан Өгүүлбэрзүй ба холбоотой объект адилтгагч (ОА)-уудыг Хавсралт А дахь ASN.1 модулиудад зааж өгсөн болно. Энэхүү тодорхойлолтыг хэрэгжүүлэхдээ атрибутын утга DirectoryString- ээс шифрлэх байгаа сонголтуудын нэгийг хэрэглэх танил бус атрибутын төрлийг (өөрөөр хэлбэл нэр залгах) боловсруулахдаа Бүлэг 7.1 дэх харьцуулах дүрмийг ашиглахаар БАЙЖ БОЛНО. Танихгүй атрибутын төрлүүд нь DirectoryString-д олдсоноос өөр шифрлэлт бүхий атрибутын утгыг агуулсан тохиолдолд хоёртын харьцуулалтыг ашиглах хэрэгтэй.

Энэ нь хэрэгжүүлэлтэд субъектийн нэр дэх танил бус атрибутуудтай гэрчилгээг боловсруулахыг зөвшөөрдөг. DirectoryString төрлийн атрибутын утгыг шифрлэх үед тохирох ГОБ нь PrintableString эсвэл UTF8String шифрлэлтийг дараах үл хамаарах зүйлүүдтэй хамт ЗААВАЛ ашиглах ёстой:

a) Гэрчилгээний субъект нь ГОБ байх үед субъект талбарыг субъект ГОБ-аар олгогдсон бүх гэрчилгээ дэх олгогч талбар (4.1.2.4)-д

шифрлэгдсэнтэй ижил аргаар ЗААВАЛ шифрлэгдсэн байна. Тиймээс, хэрэв субъект ГОБ нь TeletexString, BMPString, эсвэл UniversalString шифрлэлтүүдийг ашиглан олгох гэрчилгээнүүдийн олгогч талбар дахь атрибутуудыг шифрлэх бол ГОБ-аар олгогдсон гэрчилгээнүүдийн субъект талбар ижил шифрлэлт ЗААВАЛ ашиглана.

b) Гэрчилгээний субъект нь ХГЖ олгогч байх үед субъект талбарыг субъект ХГЖ олгогчоор олгосон бүх ХГЖ- ууд дахь олгогч талбар (5.1.2.3)-т шифрлэгдсэнтэй ЗААВАЛ ижил аргаар шифрлэсэн байх ёстой.

c) TeletexString, BMPString, болон UniversalString нь хоцрогдсон нийцтэй байхын тулд багтсан бөгөөд шинэ хичээлийн гэрчилгээнд Ашиглаж болохгүй. Гэсэн хэдий ч эдгээр төрлийг өмнө нь нэр нь бий болсон гэрчилгээнд ашиглаж болно, үүнд одоо байгаа субъектэд шинэ гэрчилгээ олгох эсвэл шифрлэгдсэн шинж чанарууд нь өмнө нь тогтоогдсон шинэ субъектэд гэрчилгээ олгох тохиолдлууд багтана. бусад субъектүүдэд олгосон гэрчилгээ. Гэрчилгээний хэрэглэгчид эдгээр төрлийн гэрчилгээ авахад бэлэн байх ёстой.

emailAddress атрибут [RFC2985] гэх субъектийн ялгах нэрд цахим шуудангийн хаягийг оруулсан тохиолдолд уламжлалт хэрэгжүүлэлт байдаг. EmailAddress-д зориулсан атрибутын утга нь PrintableString тэмдэгтийн бүлийн нэг хэсэг биш байхаар '@' тэмдэгт оруулахыг зөвшөөрөх IA5String-ийн төрөл юм. emailAddress атрибутын утгууд нь үсгийн том жижгээс хамаарахгүй (жишээ нь, "subscriber@example.com" нь "SUBSCRIBER@EXAMPLE.COM"-той ижил).

Цахим шуудангийн хаягтай шинэ гэрчилгээ үүсгэх нийцтэй хэрэгжүүлэлтүүд ЗААВАЛ rfc822Name-ийг субъектийн өөр нэрийн өргөтгөл д ашиглана. Цахим шуудангийн хаягтай шинэ гэрчилгээг үүсгэх нийцтэй хэрэгжүүлэлтүүдэд таниг чаар тодорхойлсон Субъектийн хувилбар нэрийн өргөтгөл (4.2.1.6) дэх rfc822Name-ийг заавал хэрэглэх ёстой. Субъектийн ялгах нэр дэх email Address атрибутыг нэгэн зэрэг оруулах нь уламжлалт хэрэгжүүлэлтүүд хуучирсан ч зөвшөөрөгдсөн бол дэмжих болно.

4.1.2.7. Субъектийн нийтийн түлхүүрийн мэдээлэл

Энэ талбар нь нийтийн түлхүүрийг зөөвөрлөх, түлхүүрийг ашиглах алгоритмыг тодорхойлоход ашиглагддаг (жишээ нь, RSA, DSA эсвэл Diffie-Hellman). Алгоритмыг 4.1.1.2-т заасан AlgorithmIdentifier бүтцийг ашиглан тодорхойлно. Нийтийн түлхүүрийн материалуудыг (нийтийн түлхүүр ба параметрүүдийг) шифрлэхэд зориулсан алгоритм ба аргуудад зориулсан объект адилтгагчийг [RFC3279], [RFC4055], [RFC4491]-д заасан

4.1.2.8. Өвөрмөц танигчид

Эдгээр талбарууд хэрвээ хувилбар 2 эсвэл 3 (4.1.2.1) бол ЗААВАЛ ил гарах ёстой. Хэрвээ хувилбар 1 бол эдгээр талбарууд ил гарч БОЛОХГҮЙ. Субъект болон олгогчийн өвөрмөц адилтгагчид цаг хугацааны явцад субъект ба/эсвэл олгогчийн нэрсийн дахин хэрэглэгдэх боломжтой байдлыг зохицуулахаар гэрчилгээнд дүрслэгдэнэ. Энэ профайлд нэрийг өөр нэгжүүдэд дахин ашиглаж болохгүй ба интернэтийн гэрчилгээнд өвөрмөц адилтгагч ашиглахгүй байхыг ЗӨВЛӨЖ БАЙНА. Энэ профайлд нийцсэн ГОБ нь өвөрмөц адилтгагчтай гэрчилгээ үүсгэж БОЛОХГҮЙ. Энэ профайлтай нийцсэн программууд нь өвөрмөц танигч агуулсан гэрчилгээг задлан шинжлэх чадвартай байх ХЭРЭГТЭЙ боловч өвөрмөц адилтгагчтай холбоотой боловсруулалт хийх шаардлага байхгүй

4.1.2.9. Өргөтгөлүүд

Эдгээр талбар хэрвээ хувилбар 3 (4.1.2.1) бол ЗААВАЛ ил гарах ёстой. Хэрэв энэ талбар ил байвал нэг эсвэл олон гэрчилгээний өргөтгөлүүдийн дараалал байна. Интернэт НТДБ дахь гэрчилгээний өргөтгөлүүдийн формат болон агуулгыг 4.2-т тодорхойлсон.

4.2. Гэрчилгээний өргөтгөл

X.509 хувилбар 3 гэрчилгээнд тодорхойлсон өргөтгөлүүд нь хэрэглэгчид эсвэл нийтийн түлхүүртэй нэмэлт шинж чанаруудыг холбох, ГОБ хоорондын харилцааг удирдах арга замаар хангадаг. X.509 хувилбар 3 гэрчилгээний формат нь нийгэмлэгүүдэд тухайн нийгэмлэг дотроо мэдээллээ цорын ганц байдлаар дамжуулахын тулд хувийн өргөтгөлүүдийг тодорхойлохыг зөвшөөрдөг. Гэрчилгээний өргөтгөл бүрийг чухал эсвэл чухал биш гэж нэрлэсэн байна. Гэрчилгээ ашиглаж байгаа систем нь хэрэв зөвшөөрөгдөхгүй чухал өргөтгөл эсвэл боловсруулах боломжгүй мэдээлэл агуулсан чухал өргөтгөлтэй тааралдвал уг гэрчилгээг ЗААВАЛ татгалзана. Чухал биш өргөтгөлийг зөвшөөрөхгүй бол татгалзаж БОЛНО, гэхдээ зөвшөөрсөн тохиолдолд ЗААВАЛ түүнийг боловсруулна. Дараах хэсэгт Интернэт гэрчилгээтэй хамт ашиглахыг санал болгож буй өргөтгөлүүд болон мэдээллийн стандарт байршлыг харуулав. Нийгэмлэгүүд нэмэлт өргөтгөлүүдийг ашиглахаар сонгож болно; гэхдээ ерөнхий нөхцөлд ашиглахаас сэргийлдэг аливаа чухал өргөтгөлүүдийг гэрчилгээнд тохируулахдаа болгоомжтой байх ХЭРЭГТЭЙ.

Өргөтгөл бүр OA болон ASN.1 бүтцийг агуулна. Гэрчилгээнд уг өргөтгөл харагдах тохиолдолд OA нь extnID талбар шиг харагдах бөгөөд харгалзах ASN.1 DER- ээр шифрлэсэн бүтэц нь extnValue тэмдэгт мөрийн утга болно.

Гэрчилгээнд тодорхой нэг өргөтгөлийг нэгээс олон удаа агуулж БОЛОХГҮЙ. Жишээлбэл, гэрчилгээ нь зөвхөн нэг ГОБ-ын түлхүүрийн адилтгагч өргөтгөлтэй байна. Өргөтгөл нь FALSE анхны утга бүхий бүүлийн утгыг агуулна. Өргөтгөл бүрийн текст нь энэ профайлд хамаарах ГОБ- ийн чухал талбарт зөвшөөрөгдөхүйц утгыг зааж өгдөг.

Хамаарах ГОБ-ууд түлхүүрийн адилтгагч (4.2.1.1 болон 4.2.1.2), үндсэн хязгаарлалтууд (4.2.1.9), түлхүүрийн хэрэглээ (4.2.1.3), гэрчилгээний бодлогын өргөтгөл (4.2.1.4)- үүдийг ЗААВАЛ дэмжинэ. Хэрэв ГОБ нь субъектийн талбарт хоосон цуваа бүхий гэрчилгээ олгодог бол, уг ГОБ нь субъектийн нэмэлт нэрийн өргөтгөлийг ЗААВАЛ дэмжинэ (4.2.1.6). Үлдсэн өргөтгөлүүдийг дэмжих нь ЗААВАЛ БИШ. Хамаарах ГОБ нь энэ тодорхойлолтод тодорхойлоогүй өргөтгөлүүдийг дэмжиж БОЛНО; гэрчилгээ олгогч нь эдгээр өргөтгөлүүдийг чухал гэж тэмдэглээд харилцан ажиллахад саад учруулж болохыг анхааруулсан байна.

Багадаа, энэ профайлд хамаарах программууд дараах өргөтгөлүүдийг ЗААВАЛ зөвшөөрнө: Түлхүүрийн хэрэглээ (4.2.1.3), гэрчилгээний бодлого (4.2.1.4), субъектийн нэмэлт нэр (4.2.1.6), үндсэн хязгаарлалтууд (4.2.1.9), нэрийн хязгаарлалтууд, (4.2.1.10), бодлогын хязгаарлалтууд (4.2.1.11), өргөтгөсөн түлхүүрийн хэрэглээ (4.2.1.12), болон хориглох anyPolicy (4.2.1.14).

Түүнээс гадна энэ профайлд хамаарах программууд нь гэрчилгээ олгогч болон субъектийн түлхүүрийн адилтгагч (4.2.1.1 болон 4.2.1.2), бодлогын зураглал (4.2.1.5) өргөтгөлүүдийг зөвшөөрөх ХЭРЭГТЭЙ.

4.2.1 Стандарт өргөтгөлүүд

Энэ хэсэгт [X.509]-д тодорхойлсон Интернэтийн нийтийн түлхүүрийн дэд бүтцэд ашиглах стандарт гэрчилгээний өргөтгөлүүдийг тодорхойлно. Өргөтгөл бүр [X.509]- д тодорхойлсон OA-тэй холбоотой. Эдгээр OA нь дараах байдлаар тодорхойлогддог id-cearc-ийн гишүүд байна:

4.2.1.1. Гэрчилгээ олгох байгууллагын түлхүүрийн адилтгагч

Гэрчилгээ олгох байгууллагын түлхүүрийн адилтгагчийн өргөтгөл нь гэрчилгээнд зурагдсан хувийн түлхүүрт харгалзах нийтийн түлхүүрийг таних үүргээр хангана. Уг өргөтгөл нь гэрчилгээ олгогч олон гарын үсэг зурах түлхүүр эзэмшдэг тохиолдолд (олон зэрэг түлхүүрийн хос эсвэл өөрчлөлтийн улмаас) ашиглагддаг. Адилтгал нь түлхүүрийн адилтгагч (гэрчилгээ олгогчийн гэрчилгээ дэх субъектийн түлхүүрийн адилтгагч) эсвэл гэрчилгээ олгогчийн нэр, сериал дугаарын аль нэг дээр суурилж болно.

Гэрчилгээний шатлалыг үүсгэхэд хялбар болгохын тулд хамаарах ГОБ-аар үүсгэгдсэн бүх гэрчилгээнд authorityKeyIdentifier өргөтгөлийн keyIdentifier талбар ЗААВАЛ агуулагдаж байна. Нэг онцгой нөхцөл байна; ГОБ нь "өөрөө өөртөө гарын үсэг зурсан" гэрчилгээний хэлбэрээр нийтийн түлхүүрээ түгээдэг бол ГОБ-ын түлхүүрийн адилтгагчийг орхисон байж БОЛНО. "Өөрөө өөртөө гарын үсэг зурсан" гэрчилгээний гарын үсэг нь гэрчилгээний субъектийн нийтийн түлхүүртэй хамааралтай хувийн түлхүүрийг ашиглан үүсгэгдэнэ. (Энэ нь гэрчилгээ олгогч нийтийн болон хувийн түлхүүрүүдийг хоёуланг нь эзэмшдэг болохыг батална.) Энэ тохиолдолд субъектийн болон ГОБ-ын түлхүүрийн адилтгагч нь төсөөтэй байх боловч гэрчилгээний шатлалыг байгуулахад зөвхөн субъектийн түлхүүрийн адилтгагч шаардлагатай.

keyIdentifier талбарын утгыг гэрчилгээний гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүр эсвэл цорын ганц утгыг үүсгэх аргаар гарган авах ХЭРЭГТЭЙ. Нийтийн түлхүүрээс түлхүүрийн адилтгагчийг үүсгэх хоёр нийтлэг аргыг 4.2.1.2- д тодорхойлсон. Түлхүүрийн адилтгагчийн өмнө нь тодорхойлоогүй тохиолдолд keyIdentifiers үүсгэх эдгээр аргуудын нэгийг ашиглах эсвэл ялгаатай хаш алгоритм ашигладаг ижил төрлийн аргыг ашиглахыг энэ тодорхойлолт нь ЗӨВЛӨЖ байна. Хэрэв түлхүүрийн адилтгагчийг өмнө нь тодорхойлсон тохиолдолд уг ГОБ өмнө нь тодорхойлсон адилтгагчийг ашиглах хэрэгтэй.

Энэ профайл бүх гэрчилгээ хэрэглэгчид түлхүүрийн адилтгагчийн аргыг дэмжихийг ЗӨВЛӨЖ байна.

Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал биш гэж тэмдэглэнэ.

```
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE {
  keyIdentifier             [0] KeyIdentifier            OPTIONAL,
  authorityCertIssuer       [1] GeneralNames             OPTIONAL,
  authorityCertSerialNumber [2] CertificateSerialNumber  OPTIONAL  }

KeyIdentifier ::= OCTET STRING
```

4.2.1.2. Субъектийн түлхүүрийн адилтгагч

Субъектийн түлхүүрийн адилтгагч өргөтгөл нь тодорхой нийтийн түлхүүр агуулсан гэрчилгээг таних үүргээр хангана.

Гэрчилгээний шатлалыг үүсгэхэд хялбар болгохын тулд энэ өргөтгөл нь бүхий л хамаарах ГОБ-ын гэрчилгээнд ЗААВАЛ харагдана. Өөрөөр хэлбэл, бүх

гэрчилгээ сА- ийн утга ҮНЭН байх үндсэн хязгаарлалтын өргөтгөл (4.2.1.9)-ийг агуулж байна. Хамаарах ГОБ-ын гэрчилгээнүүдэд субъектийн түлхүүрийн адилтгагчийн утга нь ЗААВАЛ уг гэрчилгээний субъектийн олгогдсон гэрчилгээний ГОБ-ын түлхүүрийн адилтгагч өргөтгөлийн түлхүүрийн адилтгагч талбарт байрших утга байна. Программууд гэрчилгээний шатлалыг шалгах үед түлхүүрийн адилтгагч таарч байгаа эсэхийг баталгаажуулах шаардлагагүй.

ГОБ-ын гэрчилгээнд субъектийн түлхүүрийн адилтгагчуудыг нийтийн түлхүүр эсвэл цорын ганц утга үүсгэх аргаас гаргаж авах ХЭРЭГТЭЙ. Нийтийн түлхүүрээс түлхүүрийн адилтгагч үүсгэх хоёр нийтлэг арга байдаг:

1) keyIdentifier нь subjectPublicKey битийн цуваа бүхий 160-бит SHA-1 хэш утгаас (tag, урт, unused bits- ийн тоо зэргээс гадна) бүрдэнэ.
2) keyIdentifier нь 0100 утгатай дөрвөн бит төрлийн талбараас бүрдэх бөгөөд үүний дараа subjectPublicKey битийн цуваа бүхий тодорхой 60 битийн SHA-1 хэшийн утга байна.

Цорын ганц тоо үүсгэх бусад аргууд мөн зөвшөөрөгдөнө.

Эцсийн объектын гэрчилгээнд, субъектийн түлхүүрийн адилтгагч өргөтгөл нь программд ашиглагдаж байгаа тодорхой нийтийн түлхүүрийг агуулж байгаа гэрчилгээг таних хэрэгслээр хангадаг. Эцсийн объект нь хэд хэдэн ГОБ-аас хэд хэдэн гэрчилгээ авсан тохиолдолд субъектийн түлхүүрийн адилтгагч нь тодорхой нийтийн түлхүүр агуулж байгаа багц гэрчилгээг хурдан таних боломжоор хангана. Зохих эцсийн объектын гэрчилгээг баталгаажуулахад программуудад туслахын тулд энэ өргөтгөл нь бүх эцсийн объектын гэрчилгээнд агуулагдаж байх ХЭРЭГТЭЙ.

Эцсийн объектын гэрчилгээнд субъектийн түлхүүрийн адилтгагчийг нийтийн түлхүүрээс гаргаж авах ХЭРЭГТЭЙ. Нийтийн түлхүүрээс түлхүүрийн адилтгагчийг үүсгэх хоёр нийтлэг аргыг дээр дурдсан байгаа.

Хэрэв түлхүүрийн адилтгагчийг урьдчилан тодорхойлоогүй бол энэ тодорхойлолт нь keyIdentifiers үүсгэх эдгээр аргуудын нэгийг ашиглах эсвэл ялгаатай хэш алгоритм ашигладаг ижил аргуудыг хэрэглэхийг ЗӨВЛӨЖ байна. Түлхүүрийн адилтгагчийг өмнө нь тодорхойлсон бол ГОБ өмнө нь тодорхойлсон адилтгагчийн ашиглах ХЭРЭГТЭЙ.

Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал биш гэж тэмдэглэнэ.

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER  ::=  { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier
```

4.2.1.3. Түлхүүрийн хэрэглээ

Түлхүүрийн хэрэглээний өргөтгөл нь гэрчилгээнд агуулагдах түлхүүрийн зорилгыг тодорхойлно (жишээлбэл нууцлал, гарын үсэг, гэрчилгээнд гарын үсэг зурах). Нэгээс олон үйлдэлд ашиглаж болох түлхүүрийг хязгаарлах тохиолдолд хэрэглээний хязгаарлалтыг ашиглаж болно. Жишээлбэл, RSA түлхүүрийг зөвхөн нийтийн түлхүүрийн гэрчилгээ болон ХГЖ-ээс бусад объектууд дээрх гарын үсгийг шалгах үед digitalSignature ба/эсвэл nonRepudiation битийг баталгаажуулахад ашиглах хэрэгтэй. Түүнчлэн RSA түлхүүрийг зөвхөн түлхүүрийн менежментэд ашиглах тохиолдолд keyEncipherment битийг баталгаажуулах болно.

Хамаарах ГОБ-ууд уг өргөтгөлийг бусад нийтийн түлхүүрийн гэрчилгээ эсвэл ХГЖ дээр тоон гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүр агуулсан гэрчилгээнд ЗААВАЛ оруулна. Байгаа тохиолдолд хамаарах ГОБ-ууд уг өргөтгөлийг чухал гэж тэмдэглэх ХЭРЭГТЭЙ.

```
id-ce-keyUsage OBJECT IDENTIFIER  ::=  { id-ce 15 }

KeyUsage ::= BIT STRING  {
    digitalSignature        (0),
    nonRepudiation          (1),- - recent editions of X.509 have
                  - - renamed  this bit to contentCommitment
    keyEncipherment         (2),
    dataEncipherment        (3),
    keyAgreement            (4),
    keyCertSign             (5),
    cRLSign                 (6),
    encipherOnly            (7),
    decipherOnly            (8) }
```

KeyUsage төрлийн битүүдийг дараах байдлаар ашигладаг:

Объектын баталгаажуулалтын үйлчилгээ, өгөгдлийн гарал үүслийн баталгаажуулалтын үйлчилгээ эсвэл бүрэн бүтэн байдлын үйлчилгээ гэх мэт гэрчилгээ дээрх гарын үсэг (5 бит) болон ХГЖ (6 бит)-ээс бусад тоон гарын үсгийг шалгахад субъектийн нийтийн түлхүүрийг ашиглахад digitalSignature битийг баталгаажуулна.

Гэрчилгээ дээрх гарын үсэг (5 бит) болон ХГЖ (6 бит)- ээс бусад тоон гарын үсгийг шалгахад тухайн субъектийн нийтийн түлхүүрийг ашиглах үед nonRepudiation битийг баталгаажуулж, гарын үсэг зурсан этгээд зарим

үйлдлийг худал үгүйсгэхээс хамгаална. Дараа нь зөрчил гарсан тохиолдолд найдвартай гуравдагч этгээд гарын үсэг зурсан мэдээллийн үнэн зөвийг тодорхойлж болно. (X.509-ийн сүүлийн хэвлэлүүдэд nonRepudiation битийн нэрийг contentCommitment болгон өөрчилсөн болохыг анхаарна уу.)

Субъектийн нийтийн түлхүүр нь хувийн эсвэл нууц түлхүүрийг шифрлэхэд өөрөөр хэлбэл түлхүүрийг дамжуулах үед ашиглахад keyEncipherment битийг баталгаажуулна. Жишээлбэл, RSA нийтийн түлхүүр нь тэгш хэмт агуулгыг-задлах түлхүүр эсвэл тэгш хэмт бус хувийн түлхүүрийг шифрлэхэд ашиглагдах үед энэ битийг тохируулах ёстой.

Субъектийн нийтийн түлхүүр нь хэрэглэгчийн түүхий өгөгдлийг дундын тэгш хэмт шифрлэлт ашиглахгүйгээр шууд шифрлэж байгаа тохиолдолд dataEncipherment битийг баталгаажуулна. Энэ битийн хэрэглээ маш ховор; ерөнхийдөө ихэнх программ тэгш хэмтэй түлхүүрийг бий болгохын тулд түлхүүрийн дамжуулалт эсвэл түлхүүрийн хэлэлцээрийг ашигладаг.

Субъектийн нийтийн түлхүүрийг түлхүүрийн хэлэлцээрт ашиглах үед keyAgreement битийг баталгаажуулна. Жишээлбэл, түлхүүрийн менежментэд Диффе-Хеллман түлхүүрийг ашиглах үед энэ битийг тохируулна.

Субъектийн нийтийн түлхүүрийг нийтийн түлхүүрийн гэрчилгээ дээрх гарын үсгийг баталгаажуулахад ашигласан тохиолдолд keyCertSign битийг баталгаажуулна. Хэрэв keyCertSign бит баталгаажсан бол үндсэн хязгаарлалтын өргөтгөлийн (4.2.1.9) cA битийг мөн ЗААВАЛ баталгаажуулна.

Субъектийн нийтийн түлхүүрийг гэрчилгээний хүчингүй жагсаалт дээрх гарын үсгийг шалгахад ашиглавал cRLSign битийг баталгаажуулна (жишээ нь, ХГЖ, дельта ХГЖ эсвэл ARLs).

keyAgreement бит байхгүй тохиолдолд encipherOnly битийн утга тодорхойгүй байна. keyAgreement битийг тохируулж, encipherOnly битийг баталгаажуулсан тохиолдолд субъектийн нийтийн түлхүүрийг зөвхөн түлхүүрийн хэлэлцээр гүйцэтгэх явцад өгөгдлийг шифрлэхэд ашиглаж болно.

keyAgreement бит байхгүй тохиолдолд decipherOnly битийн утга тодорхойгүй байна. decipherOnly бит баталгаажсан, keyAgreement битийг мөн тохируулсан тохиолдолд субъектийн нийтийн түлхүүрийг зөвхөн түлхүүрийн хэлэлцээр гүйцэтгэх явцад өгөгдлийн шифрийг тайлахад ашиглаж болно.

Хэрэв keyUsage өргөтгөл байгаа бол харгалзах keyCertSign эсвэл cRLSign битийг тохируулахгүйгээр субъектийн нийтийн түлхүүрийг ХГЖ эсвэл гэрчилгээ дээрх гарын үсгийг шалгахад ашиглаж БОЛОХГҮЙ. Хэрэв субъектийн нийтийн

түлхүүр нь зөвхөн гэрчилгээ эсвэл ХГЖ дээрх гарын үсгийг шалгахад ашиглах бол digitalSignature болон nonRepudiation битүүдийг тохируулах ХЭРЭГГҮЙ. Гэсэн хэдий ч, хэрэв субъектийн нийтийн түлхүүрийг гэрчилгээ эсвэл ХГЖ болон бусад объектууд дээрх гарын үсгийг шалгахад ашиглах бол keyCertSign болон/эсвэл cRLSign битүүдээс гадна digitalSignature болон/эсвэл nonRepudiation битүүдийг тохируулж БОЛНО.

keyUsage гэрчилгээний өргөтгөлд nonRepudiation битийг бусад keyUsage биттэй нэгтгэх нь тухайн гэрчилгээг ашиглах нөхцөлөөс хамаарч аюулгүй байдлын үр дагавартай байж болно. Цаашид digitalSignature болон nonRepudiation битүүдийн хоорондын ялгааг тусгай гэрчилгээний бодлогод тусгаж болно.

Энэ профайл нь keyUsage өргөтгөлийн хувилбарт тохируулж битүүдийн хослолыг хязгаарладаггүй. Гэсэн хэдий ч тодорхой алгоритмуудад зориулсан keyUsage өргөтгөлүүдэд тохирох утгыг [RFC3279], [RFC4055] болон [RFC4491]-д зааж өгсөн. keyUsage өргөтгөл нь гэрчилгээнд харагдах тохиолдолд ядаж нэг битийг 1 гэж ЗААВАЛ тохируулна.

4.2.1.4. Гэрчилгээний бодлого

Гэрчилгээний бодлогын өргөтгөл нь нэгээс дээш бодлогын мэдээллийн нэр томьёоны дарааллыг агуулдаг бөгөөд тус бүр объектын адилтгагч (ОА) болон нэмэлт шалгуур үзүүлэлтээс бүрдэнэ. Нэмэлт шалгуур үзүүлэлт нь бодлогын тодорхойлолтыг өөрчлөхгүй. Гэрчилгээний бодлогын өргөтгөл дэх гэрчилгээний бодлогын ОА нэгээс их байж БОЛОХГҮЙ.

Эцсийн объектын гэрчилгээнд бодлогын мэдээллийн эдгээр нэр томьёо нь гэрчилгээг олгосон бодлого, гэрчилгээг ямар зорилгоор ашиглахыг заана. ГОБ-ын гэрчилгээний хувьд эдгээр бодлогын мэдээллийн нэр томьёо нь энэ гэрчилгээг агуулсан гэрчилгээний шатлалд багц бодлогыг хязгаарладаг. Хэрэв ГОБ нь энэ гэрчилгээг агуулсан гэрчилгээний шатлалд багц бодлогыг хязгаарлахыг хүсэхгүй байгаа бол { 2 5 29 32 0 } утгатай anyPolicy тусгай бодлогыг баталж БОЛНО.

Бодлогын тодорхой шаардлага бүхий программууд нь зөвшөөрөх бодлогын жагсаалттай байх ёстой бөгөөд гэрчилгээний бодлогын ОА-г тухайн жагсаалттай харьцуулна. Хэрэв энэ өргөтгөл чухал бол шатлалыг шалгах программ хангамж нь ЗААВАЛ уг өргөтгөлийг (шалгуур үзүүлэлтүүдийг оруулна) тайлбарлах боломжтой байх эсвэл гэрчилгээг ЗААВАЛ татгалзана.

Харилцан ажиллах чадварыг хөнгөвчлөхийн тулд энэ профайл нь бодлогын мэдээллийн нэр томьёог зөвхөн ОА-ээс бүрдэхийг ЗӨВЛӨДӨГ. Зөвхөн ОА нь

хангалтгүй тохиолдолд энэ профайл нь шалгуур үзүүлэлтүүдийн хэрэглээг энэ хэсэгт тодорхойлсон зүйлээр хязгаарлахыг хатуу санал болгож байна. Шалгуур үзүүлэлтүүдийг anyPolicy тусгай бодлоготой ашиглах тохиолдолд тэднийг энэ хэсэгт тодорхойлсон шалгуур үзүүлэлтээр ЗААВАЛ хязгаарлана. Зөвхөн шатлалыг шалгах явцын үр дүнд буцаасан тэдгээр шалгуур үзүүлэлтүүдийг авч үзнэ.

Энэ тодорхойлолт нь гэрчилгээний бодлого боловсруулагчид болон гэрчилгээ олгогчид ашиглах бодлогын шалгуур үзүүлэлтийн хоёр төрлийг тодорхойлдог. Шалгуур үзүүлэлтийн төрлүүд нь CPS Заагч болон Хэрэглэгчийн Мэдэгдлийн шалгуур үзүүлэлт юм.

CPS Заагч шалгуур үзүүлэлт нь ГОБ-аас нийтэлсэн Гэрчилгээний Дадлагын Мэдэгдэл (ГДМ)- ийн заагчийг агуулдаг. Заагч нь URI хэлбэртэй байна. Энэ шалгуур үзүүлэлтийг боловсруулах шаардлагууд нь дотоод асуудал байна. Уг өргөтгөлийн хувьд чухал утгыг баталгаажсан эсэхийг үл харгалзан энэ тодорхойлолтоор ямар нэг арга хэмжээ авах шаардлагагүй.

Хэрэглэгчийн мэдэгдэл нь гэрчилгээг ашиглах үед итгэмжлэгдсэн этгээдэд үзүүлэх зориулалтай. Зөвхөн шатлалыг баталгаажуулах явцад ирсэн хэрэглэгчийн мэдэгдлүүдийг хэрэглэгчдэд харуулах зориулалттай. Хэрэв мэдэгдэл нь давхардсан тохиолдолд зөвхөн нэг хуулбарыг харуулах шаардлагатай. Ийм давхардлаас урьдчилан сэргийлэхийн тулд энэ шалгуур үзүүлэлт нь зөвхөн эцсийн объектын гэрчилгээ болон бусад байгууллагад олгосон ГОБ-ийн гэрчилгээнд байх ХЭРЭГТЭЙ.

Хэрэглэгчийн мэдэгдэл нь нэмэлт хоёр талбартай байна: noticeRef талбар, explicitText талбар. Хамаарах ГОБ- ууд noticeRef сонголтыг ашиглах ХЭРЭГГҮЙ.

Хэрэв noticeRef талбарыг ашиглавал уг талбарт байгууллагыг нэрлэх бөгөөд тухайн байгууллагын үүсгэсэн тодорхой текст мэдэгдлийг дугаараар нь тодорхойлдог. Жишээлбэл, "CertsRUs" байгууллага, мэдэгдлийн дугаар 1 гэдгийг тодорхойлж болно. Ердийн хэрэгжилтэд, хэрэглээний програм хангамж нь CertsRU-д зориулсан одоогийн мэдэгдлийн багцыг агуулсан мэдэгдлийн файлтай байна; программ нь уг файлаас мэдэгдлийн текстийг задалж, харуулна. Мессеж нь олон хэлээр бичигдсэн БАЙЖ БОЛНО, тухайн программ хангамжид өөрийн орчинд тохирох тодорхой хэлний мессежийг сонгох боломж олгоно.

explicitText талбар нь текстийн мэдэгдлийг гэрчилгээнд шууд агуулна. explicitText талбар нь хамгийн ихдээ 200 тэмдэгттэй байна. Хамаарах ГОБ-ууд нь explicitText-д UTF8String кодчилол ашиглах ХЭРЭГТЭЙ, гэхдээ

IA5String-г ашиглаж БОЛНО. Хамаарах ГОБ-ууд explicitText- ийг VisibleString эсвэл BMPString- ээр кодолж БОЛОХГҮЙ. explicitText тэмдэгт нь дурын хяналтын тэмдэгт агуулж БОЛОХГҮЙ (жишээ нь, U+0000- ээс U+001F хүртэл, U+007F- ээс U+009F хүртэл). UTF8String кодчилол ашиглаж байгаа үед бүх тэмдэгтийн цуваа Юникод нормчлолын С хэлбэр (NFC) [NFC]- ийн дагуу нормчлогдсон байх ХЭРЭГТЭЙ.

Хэрэв noticeRef болон explicitText сонголтууд хоёулаа нэг шалгуур үзүүлэлтэд багтсан бол программ хангамж нь noticeRef сонголтоор заасан мэдэгдлийн текстийн байршлыг олох боломжтой бол уг текстийг харуулах ХЭРЭГТЭЙ. Өөрөөр хэлбэл, explicitText тэмдэгтүүд харагдаж байх ХЭРЭГТЭЙ.

Тэмдэглэл: explicitText нь хамгийн ихдээ 200 тэмдэгт боловч зарим хамааралтай биш ГОБ-ууд энэ хязгаараас хэтэрсэн байдаг. Тиймээс гэрчилгээний хэрэглэгчид 200-аас дээш тэмдэгт бүхий explicitText- тэй ажиллах ХЭРЭГТЭЙ.

```
id-ce-certificatePolicies OBJECT IDENTIFIER  ::=  { id-ce 32 }

anyPolicy OBJECT IDENTIFIER  ::= { id-ce-certificatePolicies 0 }

certificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier   CertPolicyId,
    policyQualifiers   SEQUENCE SIZE (1..MAX) OF
                        PolicyQualifierInfo OPTIONAL  }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId  PolicyQualifierId,
    qualifier          ANY  DEFINED BY policyQualifierId }
```

-- Интернэт бодлогын шалгуур үзүүлэлтүүдэд зориулсан policyQualifierIds

```
id-qt          OBJECT IDENTIFIER  ::=  { id-pkix 2 }
id-qt-cps      OBJECT IDENTIFIER  ::=  { id-qt 1 }
id-qt-unotice  OBJECT IDENTIFIER  ::=  { id-qt 2 }

PolicyQualifierId ::= OBJECT IDENTIFIER  ( id-qt-cps | id-qt-unotice )

Qualifier ::= CHOICE  {
    cPSuri           CPSuri,
    userNotice       UserNotice }
```

```
CPSuri ::= IA5String

UserNotice ::= SEQUENCE {
    noticeRef        NoticeReference OPTIONAL,
    explicitText     DisplayText OPTIONAL }

NoticeReference ::= SEQUENCE {
    organization     DisplayText,
    noticeNumbers    SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
    ia5String        IA5String      (SIZE (1..200)),
    visibleString    VisibleString  (SIZE (1..200)),
    bmpString        BMPString      (SIZE (1..200)),
    utf8String       UTF8String     (SIZE (1..200)) }
```

4.2.1.5. Бодлогын зураглал

ГОБ-ийн гэрчилгээнд энэ өргөтгөлийг ашигладаг. Энэ нь нэгээс олон ОА-ын хосыг жагсааж; хос тус бүр нь issuerDomainPolicy болон subjectDomainPolicy агуулдаг. Хосолсон байдал нь гэрчилгээ олгож байгаа ГОБ-ын issuerDomainPolicy-ийг субъектийн ГОБ-ын subjectDomainPolicy-тэй адил гэж үзнэ гэдгийг илэрхийлнэ.

Гэрчилгээ олгож байгаа ГОБ-ын хэрэглэгчид тодорхой программуудад issuerDomainPolicy-г зөвшөөрч болно. Бодлогын зураглал нь issuerDomainPolicy-тэй харьцуулах боломжтой байх субъектийн ГОБ-тай холбоотой бодлогын жагсаалтын тодорхойлдог. Бодлогын зураглалын өргөтгөлд нэрлэсэн issuerDomainPolicy бүрийг ижил гэрчилгээ дэх гэрчилгээний бодлогын өргөтгөлд баталгаажуулах ХЭРЭГТЭЙ. Бодлогууд нь anyPolicy (4.2.1.4) тусгай утга руу эсвэл тусгай утгаар дүрслэгдэж БОЛОХГҮЙ.

Ерөнхийдөө, бодлогын зураглалын өргөтгөлийн issuerDomainPolicy талбарт харагдаж байгаа гэрчилгээний бодлогыг гэрчилгээний шатлалын дараагийн гэрчилгээнд оруулахад зөвшөөрөгдөх бодлого гэж үзэхгүй. Зарим тохиолдолд ГОБ нь нэг бодлогыг (p1) нөгөө бодлого руу (p2) буулгахыг хүсэж болох ч, issuerDomainPolicy (p1)-ийг дараагийн гэрчилгээнүүдэд оруулахад зөвшөөрөгдөхүйц гэж үзнэ. Жишээлбэл, хэрэв бодлого p1-ийн хэрэглээнээс бодлого p2-ийн хэрэглээ рүү шилжих явцад ГОБ нь бодлого тус бүрийн дагуу олгогдсон хүчинтэй гэрчилгээтэй байна. Гэрчилгээ олгосон ГОБ-ын гэрчилгээнд хоёр бодлогын зураглалыг оруулснаар ГОБ нь үүнийг илэрхийлж болно.

Бодлогын зураглал бүр p1-ийн issuerDomainPolicy- тэй; нэг бодлогын зураглал нь p1-ийн subjectDomainPolicy- тэй, бусад нь p2-ийн subjectDomainPolicy- тэй байна.

Энэ өргөтгөлийг ГОБ- ууд болон программууд ДЭМЖИЖ БОЛНО.

Хамаарах ГОБ-ууд энэ өргөтгөлийг чухал гэж тэмдэглэх ХЭРЭГТЭЙ.

```
id-ce-policyMappings OBJECT IDENTIFIER  ::=  { id-ce 33 }

PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy      CertPolicyId,
    subjectDomainPolicy     CertPolicyId }
```

4.2.1.6. Субъектийн нэмэлт нэр

Субъектийн нэмэлт нэрийн өргөтгөл нь адилтгалыг гэрчилгээний субъект руу холбох боломжийг олгодог. Эдгээр адилтгалуудыг гэрчилгээний субъектийн талбарт адилтгалын оронд эсвэл нэмэлтээр оруулж болно. Тодорхойлогдсон сонголтуудад Интернэт цахим шуудангийн хаяг, DNS нэр, IP хаяг болон Uniform Resource Identifier (URI)- ийг оруулна. Зөвхөн дотроо тодорхойлсон бусад сонголтууд байгаа. Олон нэрийн хэлбэр болон нэрийн хэлбэр бүрийн олон тохиолдлыг агуулж БОЛНО. Ийм адилтгалыг гэрчилгээнд оруулах бүрд субъектийн нэмэлт нэрийн (эсвэл гэрчилгээ олгогчийн нэмэлт нэр) өргөтгөлийг ЗААВАЛ ашигласан байна; гэхдээ 4.1.2.4 хэсэгт тодорхойлсон шиг domainComponent шинж чанарыг ашиглан субъектийн талбарт DNS нэрийг мөн дүрсэлж болно. Субъектийн талбарт ийм нэрийг илэрхийлсэн тохиолдолд тэдгээрийг DNS нэр рүү хөрвүүлэх шаардлагагүй гэдгийг анхаарна уу.

Учир нь субъектийн нэмэлт нэрийг нийтийн түлхүүртэй тодорхой холбоотой гэж үздэг тул субъектийн нэмэлт нэрийн бүх хэсэг нь ГОБ-аар ЗААВАЛ баталгаажсан байна.

Цаашилбал, хэрэв гэрчилгээнд орсон цорын ганц субъектийн адилтгал нь нэмэлт нэрийн хэлбэр (жишээ нь, цахим шуудангийн хаяг) бол тухайн субъектийн ялгах нэр нь ЗААВАЛ хоосон (хоосон дараалал) байх бөгөөд subjectAltName өргөтгөл ЗААВАЛ байна. Хэрэв субъектийн талбар хоосон цуваа агуулсан байвал гэрчилгээ олгож байгаа ГОБ нь чухал гэж тэмдэглэсэн subjectAltName өргөтгөлийг ЗААВАЛ агуулна. subjectAltName өргөтгөл нь хоосон биш субъектийн ялгах нэртэй гэрчилгээнд агуулагдаж байгаа үед хамаарах ГОБ- ууд subjectAltName өргөтгөлийг чухал биш гэж тэмдэглэх ХЭРЭГТЭЙ.

subjectAltName өргөтгөл нь интернэтийн шуудангийн хаягийг агуулах үед, тухайн хаягийг rfc8222Name- д ЗААВАЛ хадгалсан байна. rfc822Name- ийн формат нь [RFC2821]- ийн 4.1.2- д тодорхойлсноор “Mailbox” байна. Mailbox нь "Local-part@Domain" хэлбэртэй байна. Mailbox-т өмнө нь нэршил (ерөнхий нэр) байхгүй, төгсгөлд нь тайлбар (хаалтаар хүрээлэгдсэн бичвэр) байхгүй, "<" болон ">"- ээр хүрээлээгдээгүй байхыг анхаарна уу. Олон улсын домэйн нэрийг агуулсан Интернэт шуудангийн хаягийг шифрлэх дүрмийг 7.5- д зааж өгсөн.

subjectAltName өргөтгөл iPAddress-ийг агуулж байгаа үед уг хаяг [RFC791]- д заасны дагуу ЗААВАЛ "network byte order"- ийн октет мөрд хадгалагдаж байна. Октет бүрийн хамгийн бага жинтэй код (least significant bit (LSB)) нь сүлжээний хаягийн харгалзах байтын ХБЖК байна. IPv4- ийн хувьд [RFC791]- д заасны дагуу октет мөр ЗААВАЛ 4 октетоос бүрдэнэ. IPv6- ийн хувьд [RFC2460]- д заасны дагуу ЗААВАЛ 16 октетоос бүрдэнэ.

subjectAltName өргөтгөл домэйн нэрийн системийн нэршил агуулж байгаа тохиолдолд домэйн нэр dNSName (an IA5String)- д ЗААВАЛ хадгалагдсан байна. [RFC1034]- ийн 3.5- д заасны дагуу, [RFC1123]- ийн 2.1- д өөрчлөлт орсны дагуу тухайн нэр нь ЗААВАЛ “баримталдаг нэрийн синтакс”- д байна. Домэйн нэрд том, жижиг үсгээр бичихийг зөвшөөрдөг ч энэ тохиолдолд хамааралгүй гэдгийг анхаарна уу. Түүнээс гадна “ ” тэмдэгт нь хууль ёсны домэйн нэр байх үед “ ”-ийн dNSName- тэй subjectAltName өргөтгөлийг хэрэглэж БОЛОХГҮЙ. Төгсгөлд нь Интернэт шуудангийн хаяг (subscriber@example.com- ийн оронд subscriber.example.com) DNS илэрхийлэл хэрэглэсэн бол ашиглаж БОЛОХГҮЙ; ийм адилтгагчийг rfc822Name- ээр шифрлэсэн байна. Олон улсын домэйн нэрийг шифрлэх дүрмийг 7.2- д зааж өгсөн.

subjectAltName өргөтгөл нь URI- ийг агуулсан тохиолдолд тухайн нэр нь uniformResourceIdentifier (an IA5String)- д ЗААВАЛ хадгалагдсан байна. Уг нэр нь хамааралтай URI байж БОЛОХГҮЙ бөгөөд ЗААВАЛ

URI- ийн синтакс болон [RFC3986]- д заасан шифрлэх дүрмийг баримталсан байна. Уг нэр нь схем (жишээ нь, "http" эсвэл "ftp") болон схемийн тусгай хэсэг (scheme-specific-part) хоёуланг ЗААВАЛ агуулна. ГОБ-ыг агуулдаг URI нь ([RFC3986], 3.2) бүрэн тодорхойлогдсон домэйн нэр эсвэл хостын IP хаягийг ЗААВАЛ агуулдаг. Олон Улсын Нөөцийн Танигч (ОУНТ)- ээр шифрлэх дүрмийг 7.4- т зааж өгсөн.

[RFC3986]-д заасны дагуу схемийн нэр нь том жижиг үсэг хамаарахгүй (жишээ нь, "http" нь "HTTP"-тэй ижил). Хостын хэсэг байгаа бол мөн том жижиг үсэг хамаарахгүй, гэхдээ схемийн тусгай хэсэг (scheme-specific-part)-ийн бусад

бүрэлдэхүүнд том жижиг үсэг хамааралтай байж болно. URI- ийг харьцуулах дүрмийг 7.4- т зааж өгсөн.

subjectAltName өргөтгөл нь directoryName-дээ ЯН- г агуулж байгаа үед шифрлэх дүрмүүд 4.1.2.4- д заасан issuer талбарт тодорхойлсонтой ижил байна. Issuer талбараар тодорхойлогдсон нэг ГОБ- аар баталгаажуулсан субъект 000 (subject entity) бүрийн хувьд ЯН нь ЗААВАЛ цор ганц байна. ГОБ нь адилхан субъектийн 000 (subject entity)-д ижил ЯН- тэй нэгээс олон гэрчилгээ олгож БОЛНО.

subjectAltName нь otherName талбарыг ашиглан нэмэлт нэрийн төрлийг гаргаж БОЛНО. Нэрийн формат болон семантик нь type-id талбарын OBJECT IDENTIFIER утгаар илэрхийлэгдэнэ. Нэр нь өөрөө otherName- ийн талбарын утга болон дамжуулагдана. Жишээлбэл, Керберос 5 зарчмын нэрийн ОА болон Realm, PrincipalName- ийн ДАРААЛАЛ- ыг ашиглан Керберос [RFC4120] форматын нэрийг otherName рүү шифрлэж болно.

Субъектийн нэмэлт нэрийг 4.2.1.10- т нэрийн хязгаарлалтын өргөтгөлийг ашиглан субъектийн ялгах нэр заасан шиг ижил байдлаар хязгаарлаж БОЛНО.

Хэрэв subjectAltName өргөтгөл байгаа бол цуваа ЗААВАЛ ядаж нэг бүртгэл агуулдаг. Субъектийн талбараас ялгаатай нь хамаарах ГОБ-ууд хоосон GeneralName талбаруудыг агуулсан subjectAltNames- тэй гэрчилгээ олгож БОЛОХГҮЙ. Жишээлбэл, rfc822Name нь IA5String шиг дүрслэгдсэн. Хоосон тэмдэгт нь хүчинтэй IA5String байхад ийм rfc822Name-ийг энэ профайлаар зөвшөөрөхгүй. Гэрчилгээний шатлалыг боловсруулж байхад ийм гэрчилгээтэй тааралдах клиентийн зан төлөвийг энэ профайлаар тодорхойлоогүй болно.

Эцэст нь хөрвөх (wildcard) тэмдэгтүүд (жишээ нь, нэрийн багцын орлуулагч) агуулдаг субъектийн нэмэлт нэрийн семантикийг энэ тодорхойлолтод тусгаагүй БОЛНО. Тусгай шаардлагатай программууд ийм нэрийг ашиглаж БОЛНО, гэхдээ семантикийг тодорхойлох ёстой.

```
id-ce-subjectAltName OBJECT IDENTIFIER  ::=  { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames  ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName  ::= CHOICE  {
     otherName                  [0]    OtherName,
     rfc822Name                 [1]    IA5String,
     dNSName                    [2]    IA5String,
```

```
    x400Address                 [3]     ORAddress,
    directoryName               [4]     Name,
    ediPartyName                [5]     EDIPartyName,
    uniformResourceIdentifier   [6]     IA5String,
    iPAddress                   [7]     OCTET STRING,
    registeredID                [8]     OBJECT IDENTIFIER }

OtherName ::= SEQUENCE {
    type-id    OBJECT IDENTIFIER,
    value      [0] EXPLICIT ANY DEFINED BY type-id }

EDIPartyName ::= SEQUENCE {
    nameAssigner            [0]     DirectoryString OPTIONAL,
    partyName               [1]     DirectoryString }
```

4.2.1.7. Гэрчилгээ олгогчийн нэмэлт нэр

4.2.1.6- д зааснаар энэ өргөтгөл нь гэрчилгээ олгогчийн Интернэтийн стайл адилтгагчтай холбоотой ашиглагддаг. Гэрчилгээ олгогчийн нэмэлт нэрийг ЗААВАЛ 4.2.1.6- д заасан шиг шифрлэсэн байна. Гэрчилгээ олгогчийн нэмэлт нэр нь 6-р хэсэгт заасан гэрчилгээний шатлалыг шалгах алгоритмын нэг хэсэг болгож боловсруулаагүй болно. (Өөрөөр хэлбэл, гэрчилгээ олгогчийн нэмэлт нэрийг нэрийн хэлхээнд ашигладаггүй, нэрийн хязгаарлалтыг хэрэгжүүлдэггүй.)

Хамаарах ГОБ-ууд энэ өргөтгөлийг чухал биш гэж тэмдэглэх ХЭРЭГТЭЙ.

```
id-ce-issuerAltName OBJECT IDENTIFIER ::= { id-ce 18 }

IssuerAltName ::= GeneralNames
```

4.2.1.8. Субъектийн директор шинж

Субъектийн директор шинжийн өргөтгөл нь тухайн субъектийг адилтган таних шинжүүдийг (иргэншил гэх мэт) дамжуулахад ашигладаг. Өргөтгөл нь нэг буюу хэд хэдэн шинжийн дараалаар тодорхойлогддог. Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал биш гэж тэмдэглэнэ.

```
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= { id-ce 9 }

SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

4.2.1.9. Үндсэн хязгаарлалт

Үндсэн хязгаарлалтын өргөтгөлөөр гэрчилгээний субъект нь ГОБ уу, уг

гэрчилгээг агуулсан хүчинтэй гэрчилгээний шатлалын хамгийн гүн үү гэдгийг тодорхойлно.

CA бүүлийн утга нь баталгаажсан нийтийн түлхүүрийг гэрчилгээний гарын үсгийг шалгахад ашиглаж болох эсэхийг заана. Хэрэв cA бүүлийн утга баталгаажаагүй бол түлхүүрийн хэрэглээний өргөтгөл дэх keyCertSign битийг баталгаажуулж БОЛОХГҮЙ. Хэрэв үндсэн хязгаарлалтын өргөтгөл хувилбар 3-ийн гэрчилгээнд байхгүй эсвэл өргөтгөл байгаа боловч cA бүүлийн утга баталгаажаагүй бол баталгаажсан нийтийн түлхүүрийг гэрчилгээний гарын үсгийг шалгахад ашиглаж БОЛОХГҮЙ.

pathLenConstraint талбар нь зөвхөн cA бүүлийн утга баталгаажсан, түлхүүрийн хэрэглээний өргөтгөл байгаа бол keyCertSign бит (4.2.1.3) баталгаажсан тохиолдолд хүчин төгөлдөр болно. Энэ тохиолдолд, энэ нь хүчинтэй гэрчилгээний шатлалд энэ гэрчилгээг дагаж болох non-self-issued завсрын гэрчилгээний дээд тоог илэрхийлдэг. (Тэмдэглэл: Гэрчилгээний шатлал дах сүүлийн гэрчилгээ нь завсрын гэрчилгээ биш бол энэ хязгаарлалтад хамаарахгүй. Ихэвчлэн сүүлийн гэрчилгээ нь эцсийн объектын гэрчилгээ байдаг, гэхдээ ГОБ-ын гэрчилгээ байж болно.) pathLenConstraint 0 байх нь хүчинтэй гэрчилгээний шатлалаар non- self-issued завсрын ГОБ-ын гэрчилгээнүүд биш бол дагаж болно. Энэ нь харагдаж байгаа тохиолдолд pathLenConstraint талбар нь ЗААВАЛ тэгээс их буюу тэнцүү байна. pathLenConstraint талбар харагдахгүй бол хязгаарлалт тавихгүй.

Хамаарах ГОБ-ууд нь энэ өргөтгөлийг ЗААВАЛ гэрчилгээ дээрх тоон гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүрүүдийг агуулсан бүх ГОБ-ын гэрчилгээнүүдэд оруулдаг бөгөөд ийм гэрчилгээнд уг өргөтгөлийг чухал гэж тэмдэглэх ёстой. Энэ өргөтгөл нь гэрчилгээ дэх тоон гарын үсгийг баталгаажуулахаас зөвхөн бусад зорилгоор ашиглагддаг нийтийн түлхүүрүүдийг агуулсан ГОБ-ын гэрчилгээнүүдэд чухал эсвэл чухал биш өргөтгөл гэж харагдаж БОЛНО. Ийм ГОБ-ын гэрчилгээнд зөвхөн ХГЖ дээрх цахим гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүр болон гэрчилгээний бүртгэлийн протоколд ашигладаг түлхүүрийн менежментийн нийтийн түлхүүрийг агуулдаг. Энэ өргөтгөл нь эцсийн объектын гэрчилгээнд чухал эсвэл чухал биш өргөтгөл гэж харагдаж БОЛНО.

Түлхүүрийн хэрэглээний өргөтгөл keyCertSign битийг баталгаажаагүй, cA бүүлийн утга баталгаажаагүй бол ГОБ-ууд pathLenConstraint талбарыг агуулж БОЛОХГҮЙ.

```
id-ce-basicConstraints OBJECT IDENTIFIER  ::=  { id-ce 19 }
```

```
BasicConstraints ::= SEQUENCE {
    cA                  BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER  (0..MAX) OPTIONAL  }
```

4.2.1.10. Нэрийн хязгаарлалт

Зөвхөн ГОБ-ын гэрчилгээнд ЗААВАЛ ашиглагдах нэрийн хязгаарлалт өргөтгөл нь гэрчилгээний шатлал дах дараагийн гэрчилгээнүүдийн бүх субъектийн нэрийг байршуулах ёстой талбарыг илэрхийлнэ. Субъектийн ялгах нэр болон субъектийн нэмэлт нэрд хязгаарлалт үйлчилнэ. Зөвхөн өгөгдсөн нэрийн хэлбэрээр байгаа тохиолдолд хязгаарлалт үйлчилнэ. Хэрэв гэрчилгээнд тухайн төрлийн нэр байхгүй бол гэрчилгээ зөвшөөрөгдөнө.

Нэрийн хязгаарлалт нь өөрөө-олгосон гэрчилгээнд үйлчлэхгүй (гэрчилгээний шатлалын сүүлийн гэрчилгээ биш бол). (Энэ нь нэрийн хязгаарлалтыг ашигладаг ГОБ-уудыг түлхүүр шилжүүлэлтийг хэрэгжүүлэхийн тулд өөрөө-олгосон гэрчилгээ ашиглахаас сэргийлж чадна.)

Хязгаарлалт нь зөвшөөрөгдсөн эсвэл хасагдсан нэрийн дэд модны нэрээр тодорхойлогддог. excludedSubtrees талбарын хязгаарлалттай тохирох аливаа нэр нь excludedSubtrees байгаа мэдээллээс үл хамааран хүчингүй болно. Хамаарах ГОБ-ууд энэ өргөтгөлийг чухал гэж тэмдэглэх ёстой ба x400Address, ediPartyName эсвэл registeredID нэрийн хэлбэрүүд дээр нэрийн хязгаарлалт тавьж ХЭРЭГГҮЙ. Хамаарах ГОБ-ууд нэрийн хязгаарлалт нь хоосон цуваа байгаа тохиолдолд гэрчилгээ олгож БОЛОХГҮЙ. Өөрөөр хэлбэл, permittedSubtrees талбар эсвэл excludedSubtrees-ийн аль аль нь ЗААВАЛ байж байна.

Энэ профайлтай нийцэх Applications directoryName нэрийн хэлбэр дээр тавигдсан нэрийн хязгаарлалтыг ЗААВАЛ боловсруулах боломжтой байх бөгөөд rfc822Name, uniformResourceIdentifier, dNSName, and iPAddress нэрийн хэлбэр дээр тавигдсан нэрийн хязгаарлалт боловсруулах боломжтой байх ХЭРЭГТЭЙ. Хэрэв чухал гэж тэмдэглэгдсэн нэрийн хязгаарлалтын өргөтгөл нь тодорхой нэрийн хэлбэрт хязгаарлалт тавьдаг ба тухайн нэрийн хэлбэрийн жишээ нь субъектийн талбар эсвэл дараагийн гэрчилгээний SubjectAltName өргөтгөл дээр харагдах бөгөөд тухайн программ хязгаарлалтыг ЗААВАЛ боловсруулна эсвэл гэрчилгээг ЗААВАЛ татгалзана.

Энэ профайл дотор хамгийн бага болон их талбаруудыг аливаа нэрийн хэлбэртэй ашиглахгүй тул хамгийн бага нь ЗААВАЛ тэг байх ба хамгийн их гэж

ЗААВАЛ байхгүй байна. Гэсэн хэдий ч, хэрэв программ дараагийн гэрчилгээнд харагдах нэрийн хэлбэрийн хамгийн их эсвэл хамгийн бага бусад утгыг заасан чухал нэрийн өргөтгөлтэй таарвал программ нь эдгээр талбаруудыг ЗААВАЛ боловсруулна эсвэл гэрчилгээг ЗААВАЛ татгалзана.

URI-уудын хувьд, хязгаарлалт нь нэрийн хостын хэсэгт үйлчилнэ. Хязгаарлалт нь ЗААВАЛ бүрэн тодорхойлогдсон домэйн нэр шиг заасан байх бөгөөд хост эвсэл домэйнийг зааж БОЛНО. Жишээлбэл "host.example.com", ".example.com" байж болно. Хязгаарлалт нь цэгээр эхлэх үед энэ нь нэг болон түүнээс дээш тэмдэгтээр өргөтгөж БОЛНО. Өөрөөр хэлбэл, “.example.com” хязгаарлалтыг host.example.com болон my.host.example.com. хоёулаа хангасан байна. Гэхдээ ".example.com" хязгаарлалтыг "example.com"- оор хангахгүй байна. Хязгаарлалт нь цэгээр эхлээгүй тохиолдолд, энэ нь хостыг заана. Хэрэв uniformResourceIdentifier нэрийн хэлбэрт хязгаарлалт үйлчилж дараагийн гэрчилгээнд бүрэн тодорхойлогдсон домэйн нэрээр заасан хостын нэртэй authority component агуулаагүй uniformResourceIdentifier- тэй subjectAltName өргөтгөлийг агуулж байвал программ нь гэрчилгээг ЗААВАЛ татгалзана.

Интернэт шуудангийн хаягийн нэрийн хязгаарлалт нь тодорхой мэйлбокс, тодорхой хост дээрх бүх хаягууд эсвэл домэйний бүхий л мэйлбоксуудыг зааж өгч БОЛНО. Тодорхой мэйлбоксыг зааж өгөхийн тулд, хязгаарлалт нь бүтэн шуудангийн хаяг юм. Жишээлбэл, "root@example.com" нь "example.com" хост дээрх рүүт мэйлбоксыг заана. Тодорхой хост дээр бүх Интернэт шуудангийн хаягуудыг зааж өгөхийн тулд хязгаарлалтыг хостын нэрээр зааж өгнө. Жишээлбэл, "example.com" хязгаарлалт нь "example.com" хост дээрх дурын шуудангийн хаяг хангана. Домэйн дэх дурын хаягийг зааж өгөхийн тулд хязгаарлалтыг цэгээр эхлэхээр зааж өгнө (URI-тай ижил). Жишээлбэл, ".example.com" гэдэг нь "example.com" домэйн дэх бүх Интернэт шуудангийн хаягийг заана, гэхдээ "example.com" хост дээрх Интернэт шуудангийн хаяг биш.

DNS нэрийн хязгаарлалтууд host.example.com гэж илэрхийлдэг. Нэрийн зүүн талд тэг эсвэл илүү тэмдэгт (label) үүд нэмэх замаар үүсгэж чадах дурын DNS нэр нь нэрийн хязгаарлалтыг хангана. Жишээлбэл, www.host.example.com нь хязгаарлалтыг хангана, харин host1.example.com бол үгүй.

Цахим шуудангийн хаягийг emailAddress (4.1.2.6) төрлийн шинж чанарын субъектийн ялгах нэрд оруулдаг хуучин хэрэгжүүлэлтүүд байдаг. rfc822Name нэрийн хэлбэр дээр хязгаарлалтууд тавих тохиолдолд гэхдээ гэрчилгээ субъектийн нэмэлт нэрийг агуулаагүй тул rfc822Name хязгаарлалтыг субъектийн ялгах нэрийн emailAddress төрлийн шинж чанарт ЗААВАЛ

хэрэглэнэ. emailAddress- д зориулсан ASN.1 бичиглэл болон харгалзах ОА-г Хавсралт А-д оруулаа.

directoryName хэлбэрийн хязгаарлалтыг гэрчилгээний субъектийн талбарт (гэрчилгээ нь хоосон биш субъектийн нэр агуулж байхад) болон subjectAltName өргөтгөлийн directoryName төрлийн дурын нэрд ЗААВАЛ хэрэглэнэ. x400Address хэлбэрийн хязгаарлалтыг subjectAltName өргөтгөлийн x400Address төрлийн дурын нэрд ЗААВАЛ хэрэглэнэ.

directoryName хэлбэрийн хязгаарлалтыг хэрэгжүүлэхдээ хэрэгжүүлэлт нь ЯН шинж чанаруудыг ЗААВАЛ харьцуулдаг. Багадаа хэрэгжүүлэлт нь 7.1- д зааснаар ЗААВАЛ ЯН харьцуулах дүрмүүдийг гүйцэтгэнэ. directoryName хэлбэрийн хязгаарлалттай гэрчилгээг олгож буй ГОБ-ууд нь бүрэн ISO ЯН нэрийн харьцуулах алгоритмын хэрэгжүүлэлтэд найдах хэрэггүй. Энэ нь нэрийн хязгаарлалтыг субъектийн талбар эсвэл subjectAltName өргөтгөл дэх кодчилолтой ЗААВАЛ яг адилхан зааж өгнө гэсэн үг.

iPAddress- ийн синтакс нь ЗААВАЛ 4.2.1.6- д заасны дагуу нэрийн хязгаарлалтад тусгайлан дараах нэмэлтүүд орсон байна. IPv4 хаягуудын хувьд GeneralName-ийн iPAddress талбар нь [RFC4632] хаягийн мужийг илэрхийлэхийн тулд RFC 4632 (CIDR)-ийн хэлбэрээр кодолсон найман (8) октет агуулсан байна. IPv6 хаягуудын хувьд iPAddress талбар нь ижил хэлбэрээр кодолсон 32 октетыг агуулсан байна. Жишээлбэл, "С ангилал"- ийн дэд сүлжээний 192.0.0.0- ийн нэрийн хязгаарлалтын хувьд CIDR тэмдэглэлээр 192.0.2.0/24 (маск 255.255.255.0) гэж илэрхийлэгдэх C0 00 02 00 FF FF FF 00 октетоор илэрхийлсэн байна.

Нэрийн хязгаарлалтын шифрлэлт, боловсруулалтын нэмэлт дүрмүүдийг 7-р хэсэгт заасан байгаа.

otherName, ediPartyName болон registeredID- д зориулсан нэрийн хязгаарлалтын синтакс болон семантикийг энэ тодорхойлолтоор тодорхойлоогүй болно. Гэхдээ, бусад нэрийн хэлбэрүүдэд зориулсан нэрийн хязгаарлалтын синтакс болон семантикийг бусад баримт бичигт тодорхойлсон байж болно.

```
id-ce-nameConstraints OBJECT IDENTIFIER ::= { id-ce 30 }

NameConstraints ::= SEQUENCE {
    permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
```

```
GeneralSubtree  ::= SEQUENCE  {
    base                GeneralName,
    minimum         [0]     BaseDistance DEFAULT 0,
    maximum         [1]     BaseDistance OPTIONAL  }

BaseDistance ::= INTEGER  (0..MAX)
```

4.2.1.11. Бодлогын хязгаарлалт

Бодлогын хязгаарлалтын өргөтгөлийг ГОБ-уудад олгосон гэрчилгээнд ашиглаж болно. Бодлогын хязгаарлалтын өргөтгөл нь шатлалыг баталгаажуулахдаа хоёр аргаар хязгаарладаг. Үүнийг бодлогын зураглалыг хориглох эсвэл шатлал дээрх гэрчилгээ бүр зөвшөөрөгдөхүйц бодлогын адилтгагч агуулж байхыг шаардахад ашиглаж болно.

Хэрэв inhibitPolicyMapping талбар байгаа бол уг утга нь бодлогын зураглалыг цаашид зөвшөөрөхгүй байхаас өмнө шатлалд харагдаж болох нэмэлт гэрчилгээнүүдийн тоог заана. Жишээлбэл, нэг утга нь бодлогын зураглал нь энэ гэрчилгээний субъектээс олгогдсон гэрчилгээнүүдэд боловсруулж болох боловч уг шатлал дах нэмэлт гэрчилгээнд биш гэдгийг илэрхийлж байна.

Хэрэв requireExplicitPolicy талбар байгаа бол, requireExplicitPolicy-ийн утга нь бүх шатлалд тодорхой бодлого шаардагдахаас өмнө шатлал дээр харагдах нэмэлт гэрчилгээний тоог илэрхийлдэг. Тодорхой бодлого шаардлагатай үед шатлал дээрх бүх гэрчилгээнд гэрчилгээний бодлогын өргөтгөлд зөвшөөрөгдөх бодлогын тодорхойлогч байх шаардлагатай. Зөвшөөрөгдөх бодлогын тодорхойлогч нь гэрчилгээний шатлалын хэрэглэгчээс шаардагдах бодлогын тодорхойлогч эсвэл бодлогын зураглалаар тэнцүү гэж зарласан бодлогын танигч юм.

Хамаарах программууд ЗААВАЛ requireExplicitPolicy талбарыг боловсруулах боломжтой байх ба inhibitPolicyMapping талбарыг боловсруулах боломжтой байх ХЭРЭГТЭЙ. inhibitPolicyMapping талбарыг дэмждэг программууд policyMappings өргөтгөлийн дэмжлэгийг мөн ЗААВАЛ хэрэгжүүлдэг. Хэрэв policyConstraints өргөтгөлийг чухал гэж тэмдэглэсэн бөгөөд inhibitPolicyMapping талбар байгаа бол inhibitPolicyMapping талбарт дэмжлэг үзүүлэхгүй байгаа программууд нь гэрчилгээнээс ЗААВАЛ татгалздаг.

Бодлогын хязгаарлалт нь хоосон цуваа байвал ГОБ-ууд гэрчилгээ олгож БОЛОХГҮЙ. Өөрөөр хэлбэл, inhibitPolicyMapping талбар эсвэл requireExplicitPolicy талбар аль аль нь ЗААВАЛ бай на. Бодлогын хязгаарлалтын талбар хоосон тааралдах клиентийн зан төлөвийг энэ профайлд тусгаагүй болно.

Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал гэж тэмдэглэнэ.

```
id-ce-policyConstraints OBJECT IDENTIFIER  ::=  { id-ce 36 }

PolicyConstraints ::= SEQUENCE {
    requireExplicitPolicy          [0] SkipCerts OPTIONAL,
    inhibitPolicyMapping           [1] SkipCerts OPTIONAL  }

SkipCerts ::= INTEGER  (0..MAX)
```

4.2.1.12. Өргөтгөсөн түлхүүрийн хэрэглээ

Энэ өргөтгөл нь түлхүүрийн хэрэглээний өргөтгөлд заасан үндсэн зорилгоос гадна эсвэл оронд нь баталгаажсан нийтийн түлхүүр ашиглаж болох нэг болон хэд хэдэн зорилгыг заадаг. Ерөнхийдөө, энэ өргөтгөл нь зөвхөн эцсийн объектын гэрчилгээнд л байна. Энэ өргөтгөлийг дараах байдлаар тодорхойлно:

```
id-ce-extKeyUsage OBJECT IDENTIFIER  ::= { id-ce 37 }

ExtKeyUsageSyntax ::= SEQUENCE  SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER
```

Түлхүүр зорилтууд нь аливаа байгууллагын хэрэгцээгээр тодорхойлогдоно. Түлхүүр зорилтуудад адилтгаж байгаа объектын адилтгагч нь ЗААВАЛ IANA эсвэл ITU-T- ийн зөвлөмж X.660 [X.660]- ийн дагуу олгогдсон байна.

Энэ өргөтгөл гэрчилгээ олгогчийн сонголтоос хамаараад чухал эсвэл чухал биш байж БОЛНО.

Хэрэв энэ өргөтгөл байгаа бол гэрчилгээг ЗААВАЛ зөвхөн тодорхойлсон зорилгоор ашиглана. Төлөвлөсөн зорилго байгаа үед хэрэв олон зорилгыг зааж өгсөн бол тухайн программ заасан бүх зорилгыг зөвшөөрөх шаардлагагүй. Программуудыг ашиглаж байгаа гэрчилгээ нь өргөтгөсөн түлхүүрийн хэрэглээний өргөтгөлтэй байх ба гэрчилгээ нь тэрхүү программд зөвшөөрөгдөхүйц байхын тулд тодорхой зорилгыг тодорхойлсон байхыг шаардаж БОЛНО.

Хэрэв ГОБ ийм программуудыг хангахын тулд өргөтгөсөн түлхүүрийн хэрэглээний өргөтгөлийг агуулдаг боловч тухайн түлхүүрийн хэрэглээг хориглохыг хүсэхгүй байгаа бол ГОБ нь программуудад шаардагдах тодорхой түлхүүр зорилгоос гадна тусгай KeyPurposeId anyExtendedKeyUsage- ийг оруулж болно. Хэрэв anyExtendedKeyUsage KeyPurposeId байгаа бол хамаарах

ГОБ-ууд нь энэ өргөтгөлийг чухал гэж тэмдэглэх ХЭРЭГГҮЙ. Тодорхой зорилготой байхыг шаарддаг программууд anyExtendedKeyUsage ОА-г агуулдаг гэрчилгээнээс татгалзаж БОЛНО, гэхдээ тухайн программын тодорхой ОА биш.

Хэрэв гэрчилгээ нь түлхүүрийн хэрэглээний өргөтгөл, өргөтгөсөн түлхүүрийн хэрэглээний өргөтгөлийг хоёуланг нь агуулж байгаа бол хоёр өргөтгөлийг ЗААВАЛ бие даасан байдлаар боловсруулж, уг гэрчилгээг хоёр өргөтгөлтэй зөвхөн нийцүүлэх зорилгоор ЗААВАЛ ашигладаг. Хэрэв хоёр өргөтгөлтэй нийцэх зорилго байхгүй бол гэрчилгээг ямар нэг зорилгоор ашиглаж БОЛОХГҮЙ.

Дараах түлхүүрийн хэрэглээний зорилгуудыг тодорхойлсон байна:

```
anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }

id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }

id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 }
- - TLS WWW server authentication
- - Key usage bits that may be consistent: digitalSignature,
- - keyEncipherment or keyAgreement

id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 }
- - TLS WWW client authentication
- - Key usage bits that may be consistent: digitalSignature
- - and/or keyAgreement

id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }
- - Signing of downloadable executable code
- - Key usage bits that may be consistent: digitalSignature

id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }
- - Email protection
- - Key usage bits that may be consistent: digitalSignature,
- - nonRepudiation, and/or (keyEncipherment or keyAgreement)

id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 }
- - Binding the hash of an object to a time
- - Key usage bits that may be consistent: digitalSignature
- - and/or nonRepudiation

id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }
- - Signing OCSP responses
- - Key usage bits that may be consistent: digitalSignature
- - and/or nonRepudiation
```

4.2.1.13. ХГЖ тараах цэг

ХГЖ тараах цэгийн өргөтгөл нь ХГЖ мэдээллийг хэрхэн олж авахыг тодорхойлдог. Уг өргөтгөл нь чухал биш байх ХЭРЭГТЭЙ, гэхдээ энэ профайл нь ГОБ болон программуудаар энэ өргөтгөлийг дэмжихийг ЗӨВЛӨДӨГ. 5-р хэсэгт ХГЖ менежментийн талаар дэлгэрэнгүй авч үзнэ.

cRLDistributionPoints өргөтгөл нь DistributionPoint- ийн ДАРААЛАЛ байна. DistributionPoint нь гурван талбараас бүрддэг, тус бүр нь зайлшгүй биш: distributionPoint, reasons болон cRLIssuer. Эдгээр талбар бүр зайлшгүй биш боловч DistributionPoint нь зөвхөн reasons талбараас бүрдэж БОЛОХГҮЙ; distributionPoint эсвэл cRLIssuer талбарууд аль аль нь ЗААВАЛ байна. Хэрэв гэрчилгээ олгогч ХГЖ гэрчилгээ олгогч биш бол cRLIssuer талбар ЗААВАЛ байх ба ХГЖ гэрчилгээ олгогчийн Нэрийг агуулна. Хэрэв гэрчилгээ олгогч нь мөн ХГЖ гэрчилгээ олгогч бол хамаарах ГОБ-ууд cRLIssuer талбарыг ЗААВАЛ орхих бөгөөд distributionPoint талбарыг ЗААВАЛ агуулна.

distributionPoint талбар байгаа тохиолдолд энэ нь ерөнхий нэрийн ДАРААЛАЛ эсвэл nameRelativeToCRLIssuer- ийн дан ганц утгыг агуулна. Хэрэв DistributionPointName олон утга агуулж байвал нэр бүр нь ижил ХГЖ олж авах өөр өөр механизмыг тодорхойлдог. Жишээлбэл, ижил ХГЖ-ийг LDAP, HTTP-гээр дамжуулах татаж авах боломжтой байна.

Хэрэв distributionPoint талбар directoryName-ийг агуулдаг бол уг бүртгэлд directoryName нь холбогдох reasons- д зориулсан одоогийн ХГЖ- ийг агуулдаг бөгөөд ХГЖ-ийг холбогдох cRLIssuer олгодог. Уг ХГЖ нь certificateRevocationList эсвэл authorityRevocationList атрибутуудад хадгалагдаж болно. ХГЖ-ийг локал байдлаар тохируулсан директорийн серверээс программаар авч болно. Программын директор руу хандахад ашиглах протокол нь (жишээ нь, DAP эсвэл LDAP) дотоод асуудал байна.

Хэрэв DistributionPointName нь URI төрлийн ерөнхий нэр агуулдаг бол дараах семантикийг ЗААВАЛ авч үзнэ: URI нь холбогдох reasons- д зориулсан одоогийн ХГЖ-ийн заагч болох бөгөөд холбогдох cRLIssuer- ээр олгогдох болно. HTTP эсвэл FTP URI схем ашиглаж байгаа тохиолдолд URI нь ЗААВАЛ [RFC2585]- д заасны дагуу дан DER- ээр кодлогдсон ХГЖ-ийг заана. URI- аар дамжуулан хандсан HTTP сервер нь хариу мессежний агуулгын-төрөл гэсэн толгой талбарт медиа төрлийн application/pkix-crl- ийг зааж өгөх ХЭРЭГТЭЙ. LDAP URI схем [RFC4516]- ийг ашиглах тохиолдолд URI нь ХГЖ-ийг эзэмшиж байгаа бүртгэлийн ялгах нэрийг агуулж байгаа <dn> талбарыг ЗААВАЛ оруулж, ХГЖ

[RFC4523]- ийг хадгалдаг атрибутуудын зохих атрибутын тайлбарыг агуулсан дан <attrdesc>- ийг ЗААВАЛ оруулах бөгөөд <host>- ийг агуулах ХЭРЭГТЭЙ (жишээ нь, <ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?certificateRevocationList;binary>). <host> (жишээ нь, <ldap:///cn=CA,dc=example,dc=com?authorityRevocationList;binary>)- ийг орхих нь клиент зохих сервертэй холбогдох шаардлагатай байж магадгүй аливаа өмнөх мэдлэгт найдах нөлөөтэй. Хэрэв байгаа бол DistributionPointName нь ядаж нэг LDAP эсвэл HTTP URI агуулах ХЭРЭГТЭЙ.

Хэрэв DistributionPointName нь nameRelativeToCRLIssuer дан ганц утгыг агуулдаг бол уг утга нь ялгах нэрийн хэсгийг өгнө. Энэ хэсгийг ХГЖ гэрчилгээ олгогчийн X.500 ялгах нэрд хавсаргаж түгээлтийн цэгийн нэрийг авна. Хэрэв DistributionPoint доторх cRLIssuer талбар байгаа бол нэрийн хэсгийг түүнийг агуулах ялгах нэрд хавсаргана; эсрэг тохиолдолд нэрийн хэсэг гэрчилгээ олгогчийн ялгах нэрд хавсаргана. Хамаарах ГОБ- ууд түгээлтийн цэгийн нэрийг зааж өгөхийн тулд nameRelativeToCRLIssuer- ийг ашиглах ХЭРЭГГҮЙ. cRLIssuer нь нэгээс олон ялгах нэр агуулж байгаа тохиолдолд DistributionPointName нь нэмэлт nameRelativeToCRLIssuer- ийг ашиглаж БОЛОХГҮЙ.

Хэрэв DistributionPoint нь reasons талбарыг орхидог бол ХГЖ нь бүх reasons-д хүчингүй болсон мэдээллийг ЗААВАЛ оруулна. Энэ профайл нь reason кодоор ХГЖ-ийг хуваахын эсрэг ЗӨВЛӨДӨГ. Хамаарах ГОБ нь cRLDistributionPoints өргөтгөлийг гэрчилгээнд оруулсан тохиолдолд энэ нь ЗААВАЛ бүх reasons гэрчилгээг хамарсан ХГЖ-ийг заах ядаж нэг DistributionPoint- ийг оруулна.

cRLIssuer нь хүчингүй гэрчилгээний жагсаалтад гарын үсэг зурж, олгосон объектыг тодорхойлдог. Хэрэв байгаа бол cRLIssuer нь зөвхөн DistributionPoint-ын зааж буй CRL гэрчилгээ олгогчийн талбараас ЗААВАЛ ялгах нэрийг (ЯН) агуулна. cRLIssuer талбар дах нэрийн кодчилол нь ХГЖ гэрчилгээ олгогчийн талбар дах кодчилолтой ЗААВАЛ яг адилхан байна. Хэрэв cRLIssuer талбар агуулагдаж байгаа бол тухайн талбарт байгаа ЯН нь ХГЖ байрлаж байгаа X.500 эсвэл LDAP дериктор оролттой тохирохгүй бол хамаарах ГОБ-ууд distributionPoint талбарыг ЗААВАЛ оруулна.

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER  ::=  { id-ce 31 }

CRLDistributionPoints ::= SEQUENCE  SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
```

```
    distributionPoint       [0]     DistributionPointName OPTIONAL,
    reasons                 [1]     ReasonFlags OPTIONAL,
    cRLIssuer               [2]     GeneralNames  OPTIONAL  }

DistributionPointName ::= CHOICE  {
    fullName                [0]     GeneralNames,
    nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
ReasonFlags ::= BIT STRING  {
    unused                  (0),
    keyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6),
    privilegeWithdrawn      (7),
    aACompromise            (8) }
```

4.2.1.14. Хориотой anyPolicy

Хориотой anyPolicy өргөтгөл нь ГОБ-уудад олгосон гэрчилгээнд ашиглаж болно. Хориотой anyPolicy өргөтгөл нь { 2 5 29 32 0 } утга бүхий тусгай anyPolicy ОА-г илэрхийлэх нь дундын өөрөө өөртөө-олгосон ГОБ-ын гэрчилгээнд харагдахаас бусад гэрчилгээний бодлогуудад шууд таарахгүй. Уг утга нь anyPolicy- ийг цаашид зөвшөөрөхгүй байхаас өмнө шатлалд харагдаж болох өөрөө өөртөө-олгоогүй нэмэлт гэрчилгээний тоог илэрхийлнэ. Жишээлбэл, нэг утга нь энэ гэрчилгээний субъектээс олгосон гэрчилгээнд anyPolicy боловсруулж болохыг зааж байгаа ч уг шатлал дээрх нэмэлт гэрчилгээнд биш.

Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал гэж тэмдэглэнэ.

```
Conforming CAs MUST mark this extension as critical.

id-ce-inhibitAnyPolicy OBJECT IDENTIFIER  ::=  { id-ce 54 }

InhibitAnyPolicy ::= SkipCerts

SkipCerts ::= INTEGER  (0..MAX)
```

4.2.1.15. Шинэчилсэн ХГЖ (Дедта ХГЖ түгээлтийн цэг гэж нэрлэгддэг)

Шинэчилсэн ХГЖ өргөтгөл нь хэрхэн дельта ХГЖ мэдээллийг олж авах талаар заадаг. Уг өргөтгөл нь ЗААВАЛ чухал биш гэж хамаарах ГОБ-уудаар тэмдэглэгдсэн байна. 5-р хэсэгт ХГЖ менежментийн талаар дэлгэрэнгүй авч

үзсэн.

Энэ өргөтгөл болон cRLDistributionPoints өргөтгөлийн хувьд ижилхэн синтаксын ашигладаг ба 4.2.1.13- д тайлбарласан. Хоёр өргөтгөлүүдэд ижил зөвшил үйлчилнэ.

```
id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ce 46 }

FreshestCRL ::= CRLDistributionPoints
```

4.2.2. Хувийн Интернэтийн өргөтгөлүүд

Энэ хэсэгт Интернэт нийтийн түлхүүрийн дэд бүтцэд ашиглагдах хоёр өргөтгөлийг тодорхойлно. Эдгээр өргөтгөлүүдийг гэрчилгээ олгогч эсвэл субъектийн талаарх онлайн мэдээлэл рүү applications-ийг удирдан чиглүүлэхэд ашиглаж болно. Өргөтгөл бүр хандах аргачлал, хандах байршлын дараалал агуулдаг. Хандах аргачлал нь хүртээмжтэй байх мэдээллийн төрлийг илэрхийлэх объектын адилтгагч байна. Хандах байршил нь мэдээллийн формат, байршил, мэдээллийг олж авах арга зэргийг далд хэлбэрээр заах GeneralName байна.

Объектын адилтгагчуудыг хувийн өргөтгөлүүдэд тодорхойлсон. Хувийн өргөтгөлүүдтэй холбоотой объектын адилтгагчууд нь arc id-pkix доторх arc id-pe- ийн доор тодорхойлогддог. Интернэт нийтийн түлхүүрийн дэд бүтцэд тодорхойлсон аливаа ирээдүйн өргөтгөлүүдийг мөн arc id-pe дагуу тодорхойлсон байхыг шаардана.

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

id-pe  OBJECT IDENTIFIER  ::= { id-pkix 1 }
```

4.2.2.1. ГОБ-ын мэдээллийн хандалт

ГОБ-ын мэдээллийн хандалтын өргөтгөл нь өргөтгөлд харагдаж байгаа гэрчилгээний гэрчилгээ олгогчийн мэдээлэл, үйлчилгээнд хэрхэн хандахыг заана. Мэдээлэл болон үйлчилгээнд онлайн шалгах үйлчилгээ, ГОБ-ын бодлогын өгөгдлийг багтааж болно. (ХГЖ-ийн байршил нь энэ өргөтгөлд заагаагүй; уг мэдээлэл нь cRLDistributionPoints өргөтгөлөөр хангагдана). Энэ өргөтгөл нь эцсийн объект эсвэл ГОБ-ын гэрчилгээнд агуулагдаж болно. Хамаарах ГОБ-ууд энэ өргөтгөлийг ЗААВАЛ чухал биш гэж тэмдэглэнэ.

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER  ::= { id-pe 1 }

AuthorityInfoAccessSyntax  ::=
        SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription  ::=  SEQUENCE {
        accessMethod          OBJECT IDENTIFIER,
        accessLocation        GeneralName   }

id-ad OBJECT IDENTIFIER  ::= { id-pkix 48 }

id-ad-caIssuers OBJECT IDENTIFIER  ::= { id-ad 2 }

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

AuthorityInfoAccessSyntax дарааллын бүртгэл бүр нь энэ өргөтгөлд харагдах гэрчилгээний гэрчилгээ олгогчоос өгсөн нэмэлт мэдээллийн формат, байршлыг тодорхойлдог. Мэдээллийн төрөл, форматыг accessMethod талбараар тодорхойлно; accessLocation талбараар мэдээллийн байршлыг тодорхойлно. Уг гаргаж авах механизм нь accessMethod эсвэл accessLocation-д тодорхойлсноор байж болно.

Энэ профайл нь хоёр accessMethod OA-ыг тодорхойлдог: id-ad-caIssuers болон id-ad-ocsp.

Нийтийн түлхүүрийн гэрчилгээнд, id-ad-caIssuers OA-ийг уг өргөтгөлийг агуулсан гэрчилгээг олгосон ГОБ-д олгосон гэрчилгээний жагсаалт үед ашиглагддаг. ГОБ гэрчилгээ олгогчийн жишиг тодорхойлолт нь гэрчилгээ хэрэглэгчийн итгэмжлэгдсэн цэг дээр дуусгавар болох гэрчилгээний шатлалыг сонгоход нь туслах зорилготой юм.

accessMethod нь id-ad-caIssuers байдлаар харагдаж байх үед accessLocation талбар нь жишиг тодорхойлолтын сервер болон жишиг тодорхойлолтыг олж авах хандалтын протоколыг тодорхойлно. accessLocation талбар нь хэд хэдэн хэлбэртэй байх GeneralName-ээр тодорхойлогддог.

accessLocation нь directoryName байх тохиолдолд мэдээллийг локалаар тохируулсан ямар нэг директор серверээс программын тусламжтайгаар авна. directoryName дэх бүртгэлд [RFC4523]-д заасан crossCertificatePair, cACertificate атрибутууд дах ГОБ-ын гэрчилгээг агуулдаг. Программын директор руу хандахад ашиглах протокол нь (жишээ нь, DAP эсвэл LDAP) дотоод асуудал байна.

Мэдээлэл нь LDAP- аар хандах боломжтой тохиолдолд accessLocation нь

uniformResourceIdentifier байх ХЭРЭГТЭЙ. LDAP URI [RFC4516] нь ЗААВАЛ гэрчилгээг эзэмшиж буй бүртгэлийн ялгах нэрийг агуулсан <dn> талбарыг оруулах бөгөөд DER кодолсон гэрчилгээ эсвэл cross-certificate pairs [RFC4523]-ийг эзэмших атрибутуудын зохих атрибутын тайлбарыг жагсаасан <attributes> талбарыг ЗААВАЛ оруулах, мөн <host>- ийг агуулах ХЭРЭГТЭЙ (жишээ нь, <ldap://ldap.example.com/cn=CA,dc=example,dc=com?cACertificate;binary,crossCertificatePair;binary>). <host> (жишээ нь, <ldap:///cn=exampleCA,dc=example,dc=com? cACertificate;binary>)-ийг орхих нь клиент тохирох сервертэй холбогдохын тулд ямар нэг өмнөх мэдлэгт найдах нөлөө байна.

HTTP эсвэл FTP-ээр дамжуулан мэдээллийг ашиглах боломжтой тохиолдолд accessLocation нь ЗААВАЛ uniformResourceIdentifier байх бөгөөд URI нь [RFC2585]-д зааснаар ЗААВАЛ дан DER кодолсон гэрчилгээг эсвэл [RFC2797]-д заасны дагуу “certs-only” CMS мессеж BER, DER- ээр кодолсон гэрчилгээний цуглуулгыг ЗААВАЛ зааж өгнө.

Гэрчилгээнд хандахын тулд HTTP болон FTP дэмждэг хамаарах программууд нь DER- ээр кодлогдсон гэрчилгээг ЗААВАЛ зөвшөөрөх боломжтой байх бөгөөд “certs-only” CMS мессежийг зөвшөөрөх боломжтой байх ХЭРЭГТЭЙ.

HTTP сервер хэрэгжүүлэлт рүү URI- аар хандах нь дан DER- ээр кодолсон гэрчилгээний хариу мессежний агуулга-төрөл толгойн хэсэгт медиа төрлийн application/pkix-cert [RFC2585]-ийг зааж өгөх ХЭРЭГТЭЙ ба "certs-only" CMS мессежний хариу мессежний агуулга-төрөл толгойн хэсэгт медиа төрлийн application/pkcs7-mime [RFC2797]- ийг зааж өгөх ХЭРЭГТЭЙ. FTP- ийн хувьд дан DER- ээр кодолсон гэрчилгээ агуулсан файлын нэр нь “.cer” [RFC2585] дагавартай байх ХЭРЭГТЭЙ бөгөөд “certs-only” CMS мессежийг агуулсан талбарын нэр нь ".p7c" [RFC2797] дагавартай байх ХЭРЭГТЭЙ. Хэрэглэгчид медиа төрөл эсвэл файлын өргөтгөлийг агуулгын зөвлөмж болгон ашиглаж болно, гэхдээ серверийн хариунд зөв медиа төрөл эсвэл файлын өргөтгөл байгаа эсэхээс хамаарахгүй.

id-ad-calssuers accessLocation нэрийн хэлбэрийн семантикийг тодорхойлоогүй.

authorityInfoAccess өргөтгөл нь id-ad-calssuers accessMethod-ийн олон тохиолдлыг агуулж болно. Ялгаатай тохиолдлууд нь ижил мэдээлэлд хандах ялгаатай аргуудыг зааж болно эсвэл ятгаатай мэдээллийг зааж болно. id-ad-calssuers accessMethod арга нь ашиглагдаж байгаа үед ядаж нэг тохиолдол нь accessLocation нь HTTP [RFC2616] эсвэл LDAP [RFC4516] URI байхаар заах ХЭРЭГТЭЙ.

id-ad-ocsp OA нь Онлайн Гэрчилгээний Төлөвийн Протокол (ОГТБП) [RFC2560]-ыг ашиглаад уг өргөтгөлийг агуулсан гэрчилгээг хүчингүй болгох мэдээлэл бэлэн үед ашигладаг.

Id-ad-ocsp нь accessMethod гэж харагдаж байгаа тохиолдолд accessLocation талбар нь [RFC2560]- д тодорхойлсон conventions- ийг ашиглан ОГТБП-ийн responder-ийн байршил байна.

Нэмэлт хандалтын тодорхойлогчууд нь бусад НТДБХ тодорхойлолтуудад заасан болно.

4.2.2.2. Субъектийн мэдээллийн хандалт

Субъектийн мэдээллийн хандалтын өргөтгөл нь өргөтгөлд гарч байгаа гэрчилгээний субъектийн мэдээлэл, үйлчилгээнд хэрхэн хандахыг заана. Субъект нь ГОБ байх үед мэдээлэл болон үйлчилгээнд гэрчилгээ шалгах үйлчилгээ болон ГОБ-ын бодлогын өгөгдөл багтана. Субъект нь эцсийн объект байх үед мэдээлэл нь санал болгож буй үйлчилгээний төрөл болон тэдгээрт хэрхэн хандахыг тодорхойлно. Энэ тохиолдолд, энэ өргөтгөлийн агуулгыг тухайн үйлчилгээг дэмждэг протоколын тодорхойлолтод тодорхойлсон байна. Энэ өргөтгөл нь эцсийн объектод эсвэл ГОБ-ын гэрчилгээнд агуулагддаг байж болно. Хамаарах ГОБ-ууд энэ өргөтгөлийг чухал биш гэж тэмдэглэх ёстой.

```
id-pe-subjectInfoAccess OBJECT IDENTIFIER  ::= { id-pe 11 }

SubjectInfoAccessSyntax  ::=
        SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription  ::=  SEQUENCE {
        accessMethod          OBJECT IDENTIFIER,
        accessLocation        GeneralName   }
```

SubjectInfoAccessSyntax дарааллын бүртгэл бүр нь энэ өргөтгөл харагдаж байгаа гэрчилгээний субъектээс өгсөн нэмэлт мэдээллийн байршил болон форматыг тодорхойлдог. Мэдээллийн төрөл болон форматыг accessMethod талбараар заасан байна; accessLocation талбар нь мэдээллийн байршлыг заадаг. Уг гаргаж авах механизм нь accessMethod- оор эсвэл accessLocation - д зааснаар илэрхийлж болно.

Энэ профайл нь субъект нь ГОБ байх үед нэг хандалтын аргыг ашиглах бөгөөд субъект нь эцсийн объект байх үед нөгөө хандалтын аргыг ашигладаг болохыг тодорхойлдог. Нэмэлт хандалтын аргууд нь бусад үйлчилгээний протоколын тодорхойлолтод ирээдүйд тодорхойлж болно.

id-ad-caRepository OA нь тухайн субъект нь өөрийн гаргасан гэрчилгээг хадгалах санд нийтэлдэг ГОБ байх үед ашиглагддаг. accessLocation талбарыг GeneralName- ээр тодорхойлох бөгөөд энэ нь хэд хэдэн хэлбэртэй байж болно.

accessLocation нь directoryName байх тохиолдолд мэдээллийг локалаар тохируулсан ямар нэг директор серверээс программын тусламжтайгаар авна. Уг өргөтгөл нь ГОБ-ын гэрчилгээг зааж ашиглагдаж байгаа тохиолдолд directoryName дэх бүртгэлд [RFC4523]-д заасны дагуу crossCertificatePair, cACertificate атрибутууд дах ГОБ-ын гэрчилгээг агуулдаг. Программын директор руу хандахад ашиглах протокол нь (жишээ нь, DAP эсвэл LDAP) дотоод асуудал байна.

Мэдээлэлд LDAP-аар хандах боломжтой бол accessLocation нь uniformResourceIdentifier байх ХЭРЭГТЭЙ. LDAP URI [RFC4516] схем нь гэрчилгээг эзэмшиж байгаа бүртгэлийн ялгах нэрийг агуулж байгаа <dn> талбарыг ЗААВАЛ оруулах, DER- ээр кодолсон гэрчилгээ эсвэл cross-certificate хос [RFC4523]-ыг эзэмшдэг атрибутуудад зохих атрибутын тодорхойлолтыг жагсаадаг <attributes> талбарыг ЗААВАЛ оруулах бөгөөд <host>- ийг агуулах ХЭРЭГТЭЙ. (жишээ нь, <ldap://ldap.example.com/cn=CA, dc=example,dc=com?cACertificate;binary,crossCertificatePair;binary>). <host> (e.g., <ldap:///cn=exampleCA,dc=example,dc=com?cACertificate;binary>) - ийг орхих нь клиент зохих сервертэй холбогдох шаардлагатай байж магадгүй аливаа өмнөх мэдлэгт найдах нөлөөтэй.

HTTP эсвэл FTP-ээр дамжуулан мэдээллийг ашиглах боломжтой тохиолдолд accessLocation нь ЗААВАЛ uniformResourceIdentifier байх бөгөөд URI нь [RFC2585]-д заасны дагуу ЗААВАЛ дан DER кодолсон гэрчилгээг эсвэл [RFC2797]-д заасны дагуу “certs-only” CMS мессеж BER, DER- ээр кодолсон гэрчилгээний цуглуулгыг зааж өгнө. Гэрчилгээнд хандахын тулд HTTP болон FTP дэмждэг хамаарах програмууд нь DER- ээр кодлогдсон гэрчилгээг зөвшөөрөх боломжтой байх ёстой бөгөөд “certs-only” CMS мессежийг зөвшөөрөх боломжтой байх ХЭРЭГТЭЙ.

HTTP сервер хэрэгжүүлэлт рүү URI- аар хандах нь дан DER- ээр кодолсон гэрчилгээний хариу мессежний агуулга-төрөл толгойн хэсэгт медиа төрлийн application/pkix-cert [RFC2585]-ийг зааж өгөх ХЭРЭГТЭЙ ба "certs-only" CMS мессежний хариу мессежний агуулга-төрөл толгойн хэсэгт медиа төрлийн application/pkcs7-mime [RFC2797]- ийг зааж өгөх ХЭРЭГТЭЙ. FTP- ийн хувьд дан DER- ээр кодолсон гэрчилгээ агуулсан файлын нэр нь “.cer” [RFC2585] дагавартай байх ХЭРЭГТЭЙ бөгөөд “certs-only” CMS мессежийг агуулсан

талбарын нэр нь ".p7c" [RFC2797] дагавартай байх ХЭРЭГТЭЙ. Хэрэглэгчид медиа төрөл эсвэл файлын өргөтгөлийг агуулгын зөвлөмж болгон ашиглаж болно, гэхдээ серверийн хариунд зөв медиа төрөл эсвэл файлын өргөтгөл байгаа эсэхээс хамаарахгүй.

Бусад id-ad-caRepository accessLocation нэрийн хэлбэрүүдийн семантикийг тодорхойлоогүй.

subjectInfoAccess өргөтгөл нь id-ad-caRepository accessMethod-ийн олон тохиолдлыг агуулж болно. Ялгаатай тохиолдлууд нь ижил мэдээлэлд хандах ялгаатай аргуудыг зааж болно эсвэл ятгаатай мэдээллийг зааж болно. id-ad-caRepository accessMethod ашиглагдаж байгаа үед ядаж нэг жишээ accessLocation нь HTTP [RFC2616] эсвэл LDAP [RFC4516] URI байхаар заах ХЭРЭГТЭЙ.

id-ad-timeStamping OA нь субъект нь [RFC3161]-д тодорхойлсон Time Stamp Protocol ашиглан timestamping үйлчилгээ санал болгоход ашиглагдана. HTTP эсвэл FTP-ээр дамжуулан timestamping үйлчилгээг ашиглах боломжтой тохиолдолд accessLocation нь uniformResourceIdentifier байх ёстой. Цахим шуудан ашиглан timestamping үйлчилгээг ашиглах боломжтой тохиолдолд accessLocation нь rfc822Name байх ёстой. TCP/IP ашиглан timestamping үйлчилгээг ашиглах боломжтой тохиолдолд dNSName эсвэл iPAddress нэрийн хэлбэрийг ашиглаж болно. accessLocation- ний бусад нэрийн хэлбэрүүдийн семантик нь энэ тодорхойлолтоор тодорхойлогдоогүй.

Нэмэлт хандалтын тодорхойлогчийг бусад НТДБХ тодорхойлолтуудад тодорхойлсон байж болно.

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

id-ad-caRepository OBJECT IDENTIFIER ::= { id-ad 5 }

id-ad-timeStamping OBJECT IDENTIFIER ::= { id-ad 3 }
```

5. ХГЖ болон ХГЖ өргөтгөлийн профайл

Дээр X.509 хувилбар 2 ХГЖ профайлын нэг зорилго нь харилцан ажиллах, дахин ашиглах боломжтой Интернэтийн НТДБ-ийг бий болгоход дэмжлэг үзүүлэх юм. Энэ зорилгод хүрэхийн тулд өргөтгөлүүдийг хэрхэн ашиглах аргачлалыг тодорхойлсон бөгөөд ХГЖ- д агуулагдаж байгаа мэдээллийн nature- ийн талаар зарим таамаглалыг дэвшүүлсэн.

ХГЖ-ийг өргөн хүрээний хамтын ажиллагааны зорилго, үйл ажиллагааны болон

баталгаажуулалтын шаардлагуудын өргөн хүрээг хамарсан өргөн хүрээний программ, орчинд ашиглаж болно. Энэ профайл нь өргөн хүрээнд харилцан ажиллах чадварыг шаарддаг ерөнхий программуудын нийтлэг суурь үзүүлэлт бий болгодог. Уг профайл нь ХГЖ бүрээс хүлээж болох мэдээллийн багцыг тодорхойлдог. Мөн уг профайл нь байнга ашиглагддаг шинж чанаруудын ХГЖ доторх нийтлэг байршлыг, мөн эдгээр шинж чанаруудын нийтлэг дүрслэлийг тодорхойлдог.

ХГЖ гэрчилгээ олгогч нь ХГЖ- ийг олгоно. ХГЖ гэрчилгээ олгогч нь ГОБ эсвэл ГОБ-аас ХГЖ олгохоор зөвшөөрөгдсөн объект байна. ГОБ-ууд олгосон гэрчилгээнийхээ төлөвийн мэдээллээр хангахын тулд ХГЖ- ийг нийтэлдэг. Гэсэн хэдий ч, ГОБ нь энэ үүргээ өөр итгэмжлэгдсэн байгууллагад шилжүүлж болно.

ХГЖ бүр тодорхой хамрах хүрээтэй. ХГЖ- ийн хамрах хүрээ нь тухайн ХГЖ дээр харагдах гэрчилгээний багц байна. Жишээлбэл, хамрах хүрээ нь “Х ГОБ-аар олгогдсон бүх гэрчилгээ”, “Х ГОБ-аар олгогдсон бүх ГОБ-ын гэрчилгээ ”, “түлхүүр тохиролцох, ГОБ-ын тохиролцох шалтгаанаар хүчингүй болгосон Х ГОБ-аар олгогдсон бүх гэрчилгээ” эсвэл "Боулдерт байрлах NIST-ийн ажилтнуудад олгосон бүх гэрчилгээ" гэх мэт дурын дотоод мэдээлэлд үндэслэсэн гэрчилгээний багц байж болно.

Бүрэн ХГЖ нь тухайн хамрах хүрээний хүчингүй болгох шалтгаануудын аль нэгээр хүчингүй болсон ХГЖ хамрах хүрээний хүчингүй болсон бүх гэрчилгээг жагсаадаг. Бүрэн, бүрэн ХГЖ нь ГОБ-аас олгосон хугацаа нь дуусаагүй, ямар нэгэн шалтгаанаар хүчингүй болсон бүх гэрчилгээг жагсаадаг. (ГОБ болон ХГЖ гэрчилгээ олгогчид нэрээр тодорхойлогддог тул ХГЖ- ийн хамрах хүрээ нь ХГЖ-д гарын үсэг зурахад ашигладаг түлхүүр эсвэл гэрчилгээнд гарын үсэг зурахад ашигладаг түлхүүрүүдэд нөлөөлөхгүй гэдгийг анхаарна уу.) Хэрэв ХГЖ- ийн хамрах хүрээ нь ХГЖ гэрчилгээ олгогчоос өөр байгууллагаас олгосон нэг буюу хэд хэдэн гэрчилгээг багтаасан бол энэ нь шууд бус ХГЖ болно. Шууд бус ХГЖ-ийн хамрах хүрээ нь нэг ГОБ-аас олгосон гэрчилгээгээр хязгаарлагдах эсвэл олон ГОБ-аас олгосон гэрчилгээг багтааж болно. Хэрэв шууд бус ХГЖ гэрчилгээ олгогч нь ГОБ бол шууд бус ХГЖ- ийн хамрах хүрээ нь ХГЖ гаргагчийн олгосон гэрчилгээг мөн багтааж БОЛНО.

ХГЖ гэрчилгээ олгогч нь мөн дельта ХГЖ үүсгэж болно. Дельта ХГЖ нь зөвхөн жишиг бүрэн ХГЖ нийтлэгдсэнээс хойш хүчингүй болсон төлөв нь өөрчлөгдсөн гэрчилгээнүүдийн жагсаалтыг гаргадаг. Жишиг бүрэн ХГЖ-ийг үндсэн ХГЖ гэж нэрлэдэг. Дельта ХГЖ- ийн хамрах хүрээ нь түүний жишиг үндсэн ХГЖ- тэй

ЗААВАЛ ижил байна.

Энэ профайл нь нэг хувийн Интернэт ХГЖ өргөтгөлийг тодорхойлдог боловч дурын хувийн ХГЖ бүртгэлийн өргөтгөлийг тодорхойлоогүй.

Нэмэлт эсвэл тусгай зориулалтын шаардлага бүхий орчныг энэ профайл дээр бий болгох эсвэл орлуулж болно.

Хүчингүй болгох эсвэл гэрчилгээний статусын бусад механизмаар хангагдсан тохиолдолд хамаарах ГОБ нь ХГЖ олгох шаардлагагүй. Хэрэв ХГЖ- ийг олгосон бол ХГЖ нь ХГЖ- ийн хувилбар 2 байх ёстой, nextUpdate талбарт дараагийн ХГЖ олгох өдөр (5.1.2.5), ХГЖ дугаарын өргөтгөл (5.2.3), ГОБ-ын түлхүүрийн адилтгагчийн өргөтгөл (5.2.1)- ийг оруулна. ХГЖ- г дэмждэг хамаарах аппликэйшн нь нэг ГОБ-аас олгосон бүх гэрчилгээг хүчингүй болгох мэдээллийг агуулсан хувилбар 1 болон хувилбар 2-ын аль алиныг нь боловсруулах ШААРДЛАГАТАЙ. Хамаарах аппликэйшн нь дельта ХГЖ, шууд бус ХГЖ эсвэл нэг ГОБ-аас олгосон бүх гэрчилгээнээс бусад хамрах хүрээ бүхий ХГЖ- г боловсруулахыг шаардахгүй.

5.1. ХГЖ талбарууд

X.509 хувилбар 2 ХГЖ синтакс нь дараах шиг байна. Гарын үсгийг тооцоолохдоо гарын үсэг зурах өгөгдөл нь ASN.1 DER- ээр шифрлэсэн байна. ASN.1 DER кодчилол нь элемент бүрийн хувьд таг, урт, кодчилолын системийн утга байна.

```
CertificateList ::= SEQUENCE {
    tbsCertList         TBSCertList,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING }

TBSCertList ::= SEQUENCE {
    version              Version OPTIONAL,
                         - - if present, MUST be v2
    signature            AlgorithmIdentifier,
    issuer               Name,
    thisUpdate           Time,
    nextUpdate           Time OPTIONAL,
    revokedCertificates    SEQUENCE OF SEQUENCE {
        userCertificate        CertificateSerialNumber,
        revocationDate         Time,
        crlEntryExtensions     Extensions OPTIONAL
                               - - if present, version MUST be v2
                           } OPTIONAL,
    crlExtensions          [0] EXPLICIT Extensions OPTIONAL
```

- - if present, version MUST be v2

-- Хувилбар, хугацаа, CertificateSerialNumber, өргөтгөлүүд нь 4.1- д ASN.1-ээр тодорхойлсон.

4.1.1.2- т AlgorithmIdentifier- ийг тодорхойлсон.

Дараах зүйлд нь Интернэтийн нийтийн түлхүүрийн дэд бүтцэд X.509 хувилбар 2 ХГЖ-г хэрхэн ашиглах талаар тайлбарласан болно.

5.1.1. CertificateList талбарууд

CertificateList нь шаардлагатай гурван талбарын ДАРААЛАЛ байна. Уг талбаруудыг дараагийн дэд хэсгүүдэд дэлгэрэнгүй тайлбарлана.

5.1.1.1. tbsCertList

Дарааллын эхний талбар нь tbsCertList юм. Энэ талбарт гэрчилгээ олгогчийн нэр, олгох өдөр, дараагийн жагсаалтыг олгох өдөр, хүчингүй гэрчилгээний заавал биш жагсаалт болон ХГЖ заавал биш өргөтгөлүүд агуулагдана. Хүчингүй гэрчилгээ байхгүй үед хүчингүй гэрчилгээний жагсаалт байхгүй. Нэг болон түүнээс олон гэрчилгээ хүчингүй болсон үед хүчингүй гэрчилгээний жагсаалт дээрх бүртгэл бүр хэрэглэгчийн гэрчилгээний сериал дугаар, хүчингүй болсон өдөр, ХГЖ заавал биш өргөтгөлийн бүртгэлүүдийн дарааллаар тодорхойлогддог.

5.1.1.2. signatureAlgorithm

signatureAlgorithm талбар нь ХГЖ гэрчилгээ олгогч CertificateList- д гарын үсэг зурахад ашигласан алгоритмд зориулсан алгоритмын адилтгагчийг агуулдаг. 4.1.1.2- д тодорхойлогдсон AlgorithmIdentifier төрлийн талбар байна. [RFC3279], [RFC4055] болон [RFC4491] нь энэ тодорхойлолтод зориулсан дэмжигддэг алгоритмуудын жагсаалт боловч бусад гарын үсгийн алгоритмуудыг мөн дэмжиж БОЛНО.

Энэ талбар нь tbsCertList цуваа дах signature талбарынх шиг ЗААВАЛ ижил алгоритмын адилтгагч агуулна (5.1.2.2).

5.1.1.3. signatureValue

signatureValue талбар нь ASN.1 DER-ээр шифрлэсэн tbsCertList дээр тооцоолсон тоон гарын үсгийг агуудаг. ASN.1 DER-ээр шифрлэсэн tbsCertList нь гарын үсгийн функцийн ролт болж ашиглагддаг. Энэ гарын үсгийн утгыг BIT STRING- ээр кодолж, ХГЖ-ийн signatureValue талбарт оруулсан байна. [RFC3279], [RFC4055] болон [RFC4491]-д дэмждэг алгоритм тус бүрийн үйл

явцын талаарх дэлгэрэнгүй заасан.

ГОБ-ууд нь мөн ХГЖ гэрчилгээ олгогчид бол ХГЖ болон гэрчилгээнд цахимаар гарын үсэг зурахад нэг хувийн түлхүүр ашиглаж БОЛНО, эсвэл ХГЖ болон гэрчилгээнд цахимаар гарын үсэг зурахад тус тусад нь хувийн түлхүүр ашиглаж БОЛНО. Тус тусад нь хувийн түлхүүрүүд ажиллаж байгаа үед эдгээр хувийн түлхүүрүүдтэй холбоотой нийтийн түлхүүр тус бүрийг тусдаа гэрчилгээнд байрлуулж, нэгийг нь түлхүүрийн хэрэглээ өргөтгөлд keyCertSign битэд, нөгөөг нь түлхүүрийн хэрэглээ өргөтгөлд cRLSign битэд тохируулна (4.2.1.3). Тусдаа хувийн түлхүүрүүд ажиллаж байгаа үед ГОБ-аар олгогдсон гэрчилгээнүүд ижил ГОБ-ын түлхүүрийн адилтгагч агуулдаг, харгалзах ХГЖ- үүд нь ялгаатай ГОБ-ын түлхүүрийн адилтгагч агуулдаг. Гэрчилгээний гарын үсэг болон ХГЖ-ийн гарын үсгийг шалгахын тулд тусдаа ГОБ гэрчилгээ ашиглах нь аюулгүй байдлын шинж чанарыг сайжруулах боломжтой; гэсэн хэдий ч энэ нь программд ачаалал үүсгэж, харилцан ажиллах чадварыг хязгаарлаж магадгүй. Олон программууд гэрчилгээний шатлал үүсгэж, гэрчилгээний шатлалаа шалгадаг (6-р хэсэг). ХГЖ-ийг шалгалт нь эргээд ГОБ-ийн ХГЖ гарын үсгийг баталгаажуулах гэрчилгээнд зориулж тусдаа гэрчилгээний шатлалтыг үүсгэж, шалгахыг шаарддаг. ХГЖ-ийг шалгалтыг гүйцэтгэх программууд нь гэрчилгээ, ХГЖ- үүд ижил ГОБ-ын хувийн түлхүүрээр тоон гарын үсэг зурагдсан үед гэрчилгээний шатлалыг шалгахыг ЗААВАЛ дэмжинэ. Эдгээр программууд нь гэрчилгээнүүд, ХГЖ- үүд ялгаатай ГОБ-ын хувийн түлхүүрээр тоон гарын үсэг зурагдсан үед гэрчилгээний шатлалыг шалгахыг дэмжих ХЭРЭГТЭЙ.

5.1.2. “Гарын үсэг зурагдах” гэрчилгээний жагсаалт

Гарын үсэг зурагдах гэрчилгээний жагсаалт буюу TBSCertList нь шаардлагатай, заавал биш талбарын цуваа юм. Уг шаардлагатай талбарууд нь ХГЖ гэрчилгээ олгогч, ХГЖ- д гарын үсэг зурахад ашиглагддаг алгоритм, ХГЖ- ийг олгосон өдөр, хугацааг заана.

Заавал биш талбарууд нь ХГЖ гэрчилгээ олгогч дараагийн ХГЖ олгох өдөр, хугацаа, хүчингүй гэрчилгээний жагсаалт болон ХГЖ өргөтгөлийг агуулдаг. Хүчингүй гэрчилгээний жагсаалт нь ГОБ нь олгосон хүчинтэй хугацаа нь дуусаагүй аливаа гэрчилгээг хүчингүй болгоогүй тохиолдлыг дэмжих нь заавал биш. Энэ профайл хамаарах ХГЖ гэрчилгээ олгогчид нь бүх олгогдсон ХГЖ-уудад nextUpdate талбар, ХГЖ дугаар болон объектын түлхүүрийн адилтгагч оруулахыг шаарддаг.

5.1.2.1. Хувилбар

Уг заавал биш талбар нь шифрлэгдсэн ХГЖ-ийн хувилбарыг тодорхойлдог. Өргөтгөлийг ашиглаж байгаа тохиолдолд энэ профайлын шаардсанаар уг

талбар ЗААВАЛ байх бөгөөд хувилбар 2 гэж ЗААВАЛ зааж өгнө (бүхэл тоон утга нь 1 байна).

5.1.2.2. Гарын үсэг

Энэ талбарт ХГЖ-д гарын үсэг зурахад ашигладаг алгоритмын алгоритмын адилтгагчийг агуулна. Интернэт нийтийн түлхүүрийн дэд бүтцэд хамгийн түгээмэл гарын үсэг зурах алгоритмуудын ОА-уудыг [RFC3279], [RFC4055] болон [RFC4491]- д жагсаав.

Энэ талбар нь CertificateList цувааны signatureAlgorithm талбартай ЗААВАЛ ижил алгоритм тодорхойлогчийг агуулна (5.1.1.2 2).

5.1.2.3. Гэрчилгээ олгогчийн нэр

Гэрчилгээ олгогчийн нэр нь ХГЖ-д гарын үсэг зурж, түүнийг олгосон объектыг тодорхойлдог. Гэрчилгээ олгогчийн адилтгал нь гэрчилгээ олгогчийн талбарт зөөгдөнө. Нэмэлт нэрийн хэлбэр нь issuerAltName өргөтгөлд мөн харагдаж болно (5.2.2). Гэрчилгээ олгогчийн талбар нь хоосон биш X.500 ЯН-ийг ЗААВАЛ агуулна. Гэрчилгээ олгогчийн талбар нь X.501 төрлийн Нэрээр тодорхойлогдох ба гэрчилгээнд гэрчилгээ олгогчийн нэрийн талбарыг шифрлэх дүрмийг ЗААВАЛ баримтална(4.1.2.4).

5.1.2.4. Одоогийн шинэчлэлт

Энэ талбар нь тухайн ХГЖ-ийг олгох өдрийг заана. thisUpdate нь UTCTime эсвэл GeneralizedTime- ээр кодолсон байж болно.

Энэ профайлд хамаарч байгаа ХГЖ гэрчилгээ олгогч нь 2049 он хүртэлх хугацаанд thisUpdate-ийг ЗААВАЛ UTCTime- аар кодолно. Энэ профайлд хамаарч байгаа ХГЖ гэрчилгээ олгогч нь 2050 болон түүнээс хойших хугацаанд thisUpdate- ийг ЗААВАЛ GeneralizedTime-аар кодолно. Хамаарах программууд UTCTime эсвэл GeneralizedTime-аар кодлогдсон хугацааг ЗААВАЛ боловсруулах боломжтой байна.

UTCTime- ээр кодолсон бол thisUpdate-ийг ЗААВАЛ 4.1.2.5.1- д тодорхойлсны дагуу зааж, тайлбарлана. GeneralizedTime- ээр кодолсон бол thisUpdate-ийг ЗААВАЛ 4.1.2.5.2- т тодорхойлсны дагуу зааж, тайлбарлана.

5.1.2.5. Дараагийн шинэчлэлт

Энэ талбар нь дараагийн ХГЖ олгох хугацааг заана. Дараагийн ХГЖ нь заасан өдрөөс өмнө олгогдох шаардлагатай, гэхдээ заасан өдрөөс хойш олгогдож болохгүй. ХГЖ гэрчилгээ олгогч нь nextUpdate нь өмнөх бүх ХГЖ-тэй ижил эсвэл түүнээс хойш хугацаатай ХГЖ-ийг олгох ХЭРЭГТЭЙ. nextUpdate нь

UTCTime эсвэл GeneralizedTime- ээр кодолсон байж болно.

Хамаарах ХГЖ гэрчилгээ олгогчид бүх ХГЖ-үүдэд ЗААВАЛ nextUpdate талбарыг оруулна. TBSCertList- ийн ASN.1 синтакс нь энэ талбарыг ЗААВАЛ БИШ гэж тодорхойлоод, [X.509]- д тодорхойлсон ASN.1- ийн бүтэцтэй нийцэж байгааг анхаарна уу. nextUpdate- ийг орхигдуулсан ХГЖ-ийг боловсруулж буй клиентийн зан төлөвийг энэ профайлаар заагаагүй болно.

Энэ профайлд хамаарч байгаа ХГЖ гэрчилгээ олгогч нь 2049 он хүртэлх хугацаанд nextUpdate-ийг ЗААВАЛ UTCTime- аар кодолно. Энэ профайлд хамаарч байгаа ХГЖ гэрчилгээ олгогч нь 2050 болон түүнээс хойших хугацаанд nextUpdate-ийг ЗААВАЛ GeneralizedTime- аар кодолно. Хамаарах программууд UTCTime эсвэл GeneralizedTime-аар кодлогдсон хугацааг ЗААВАЛ боловсруулах боломжтой байна.

UTCTime-ээр кодолсон бол nextUpdate-ийг ЗААВАЛ 4.1.2.5.1- д тодорхойлсноор зааж, тайлбарласан байна. GeneralizedTime- ээр кодолсон бол nextUpdate-ийг ЗААВАЛ 4.1.2.5.2- д тодорхойлсны дагуу зааж, тайлбарлана.

5.1.2.6. Хүчингүй гэрчилгээнүүд

Хүчингүй болсон гэрчилгээнүүд байхгүй тохиолдолд хүчингүй гэрчилгээний жагсаалт ЗААВАЛ байхгүй байна. Үгүй бол, хүчингүй болсон гэрчилгээг тэдгээрийн сериал дугаараар жагсаана. ГОБ- аас хүчингүй болсон гэрчилгээг гэрчилгээний сериалын дугаараар таньдаг. Хүчингүй болгосон өдрийг заасан байна. revocationDate хугацааг ЗААВАЛ 5.1.2.4- т заасны дагуу илэрхийлсэн байна. Нэмэлт мэдээллийг ХГЖ өргөтгөлүүдэд оруулж болно; ХГЖ-ийн өргөтгөлүүдийг 5.3- т авч үзнэ.

5.1.2.7. Өргөтгөлүүд

Хэрэв хувилбар нь 2 (5.1.2.1) бол зөвхөн энэ талбар харагдана. Хэрэв уг өргөтгөл харагдаж байгаа бол энэ талбар нь нэг эсвэл хэд хэдэн ХГЖ өргөтгөлийн цуваа байна. 5.2- т ХГЖ өргөтгөлүүдийн талаар авч үзнэ.

5.2 ХГЖ өргөтгөлүүд

X.509 хувилбар 2 ХГЖ [X.509], [X9.55]- д зориулсан ANSI X9, ISO/IEC болон ITU-T- ээр тодорхойлогдсон өргөтгөлүүд нь ХГЖ-үүдтэй нэмэлт шинж чанаруудыг холбох аргуудаар хангадаг. X.509 хувилбар 2 ХГЖ-ийн формат нь нийгэмлэгүүдэд тухайн нийгэмлэг дотроо мэдээллээ цор ганц байдлаар дамжуулахын тулд хувийн өргөтгөлүүдийг тодорхойлохыг зөвшөөрдөг. ХГЖ дэх өргөтгөл бүр чухал эсвэл чухал биш гэж нэрлэсэн байна. Хэрэв ХГЖ нь программ боловсруулах боломжгүй чухал өргөтгөлийг агуулж байвал тухайн

программ гэрчилгээний төлөвийг тодорхойлохын тулд ХГЖ-ийг ашиглаж БОЛОХГҮЙ. Гэхдээ программууд зөвшөөрөлгүй чухал биш өргөтгөлүүдийг татгалзаж болно. Дараагийн дэд хэсэгт Интернэт ХГЖ-д хэрэглэгддэг тэдгээр өргөтгөлүүдийг харууллаа. Нийгэмлэгүүд энэ тодорхойлолтод тодорхойлоогүй өргөтгөлүүдийг ХГЖ-д оруулахаар сонгож болно. Гэхдээ ерөнхий нөхцөлд ашиглахаас сэргийлдэг аливаа чухал өргөтгөлүүдийг гэрчилгээнд оруулахдаа болгоомжтой байх ХЭРЭГТЭЙ.

Хамаарах ХГЖ гэрчилгээ олгогчийн олгосон бүх ХГЖ нь ГОБ-ын түлхүүрийн адилтгагч (5.2.1), ХГЖ дугаар (5.2.3) өргөтгөлүүдийг агуулах ШААРДЛАГАТАЙ.

5.2.1. ГОБ-ын түлхүүрийн адилтгагч

ГОБ-ын түлхүүрийн адилтгагчийн өргөтгөл нь ХГЖ-д зурагдсан хувийн түлхүүрт харгалзах нийтийн түлхүүрийг таних үүргээр хангана. Адилтгагч нь түлхүүрийн адилтгагч (ХГЖ гарын үсэг зурсан гэрчилгээний субъектийн түлхүүрийн адилтгагч) эсвэл гэрчилгээ олгогчийн нэр, сериал дугаар дээр тулгуурлаж болно. Уг өргөтгөл нь гэрчилгээ олгогч нь олон зэрэгцээ түлхүүрийн хос эсвэл өөрчлөлтийн улмаас нэгээс олон гарын үсэг зурах түлхүүртэй үед илүү тохиромжтой байдаг.

Хамаарах ХГЖ гэрчилгээ олгогчид ЗААВАЛ түлхүүрийн адилтгагчийн аргыг ашиглах бөгөөд олгосон бүх ХГЖ-д энэ өргөтгөл ЗААВАЛ багтах ёстой.

Энэ ХГЖ өргөтгөлийн синтаксийг 4.2.1.1- д тодорхойлсон.

5.2.2. Гэрчилгээ олгогчийн нэмэлт нэр

Гэрчилгээ олгогчийн нэмэлт нэрийн өргөтгөл нь ХГЖ гэрчилгээ олгогчтой нэмэлт адилтгагчийг холбох боломжийг олгодог. Тодорхойлогдсон сонголтуудад цахим шуудангийн хаяг (rfc822Name), DNS нэр, IP хаяг болон URI багтана. Нэрийн хэлбэрийн олон тохиолдлууд болон олон нэрийн хэлбэрүүдийг оруулж болно. Ийм адилтгагч ашиглах бүрт гэрчилгээ олгогч нэмэлт нэрийн өргөтгөлийг ЗААВАЛ ашиглах; гэсэн хэдий ч, DNS нэрийг 4.1.2.4- т тайлбарласны дагуу domainComponent шинж чанарыг (attribute) ашиглан гэрчилгээ олгогчийн талбарт илэрхийлсэн БАЙЖ БОЛНО.

Хамаарах ХГЖ гэрчилгээ олгогчид issuerAltName өргөтгөлийг чухал биш гэж тэмдэглэх ХЭРЭГТЭЙ.

4.2.1.7- д уг ХГЖ өргөтгөлийн ОА болон синтаксыг тодорхойлсон.

5.2 Хүчингүй гэрчилгээний жагсаалтын (ХГЖ)- ийн өргөтгөл

X.509-ийн хувилбар 2-ийн ХГЖ болох [X.509], [X9.55]- ийн хувьд ANSI X9,

ISO/IEC болон ITU-T гэсэн нийгэмлэгүүдийн гаргасан өргөтгөл нь ХГЖ-уудтай нэмэлт шинж чанаруудыг холбох аргуудыг тодорхойлно. Нийгэмлэгүүд рүү мэдээллийг цор ганцаар дамжуулдаг хувийн өргөтгөлийг тодорхойлох боломжийг X.509-ийн хувилбар 2-ийн ХГЖ-ийн форматтайгаар хэрэгжүүлдэг. Өргөтгөл нь чухал, чухал биш гэж зарлагдана. Аливаа ХГЖ нь тухайн аппликейшн боловсруулах боломжгүй ямар нэгэн чухал өртөлтийг агуулж байвал тухайн аппликейшн гэрчилгээнүүдийн төлөвийг тодорхойлохдоо тухайн ХГЖ-ийг хэрэглэхгүй. Гэхдээ аппликейшнүүд танигдахгүй чухал биш өргөтгөлүүдийг орхиж болно. Дараах дэд хэсгүүдэд интернэт сүлжээний ХГЖ-уудад хэрэглэгдэж буй өргөтгөлүүдийг үзүүлнэ. Эдгээр хэсгүүдэд тодорхойлогдоогүй ХБЖ-уудад өргөтгөлүүдийг сонгож оруулахыг нийгэмлэгүүд хийнэ. Гэхдээ, ерөнхий агуулгад хэрэглэгдэх боломжтой ХБЖ-уудад ямар нэг чухал өргөтгөлүүдийг оруулахдаа анхаарах хэрэгтэй.

Хамаарах гэрчилгээ олгох байгууллага (ГОБ)- уудын хувьд олгосон бүх ХГЖ-ууддаа ГОБ-ын түлхүүрийн адилтгагч (Section 5.2.1) болон тухайн ХБЖ-ын дугаар (Section 5.2.3) гэсэн өргөтгөлийг оруулах шаардлагатай.

5.2.1 ГОБ-ын түлхүүрийн адилтгагч

ГОБ-ын түлхүүрийн адилтгагч өргөтгөлөөр ХГЖ дээр гарын үсэг зурахад хэрэглэдэг хувийн түлхүүрт хамаарах нийтийн түлхүүрийг адилтган танина. ХГЖ-ын баталгаажуулагчийн гэрчилгээнд адилтган танилт нь субъект (гэрчилгээ эзэмшигч доод шатны ГОБ)-ийн түлхүүрийн адилтгагч эсвэл гэрчилгээ олгогчийн нэр болон сериал дугаарын аль аль нь байж болно. Энэ өргөтгөл нь гэрчилгээ олгогч нь нэгээс олон гарын үсгийн түлхүүртэй, хэд хэдэн түлхүүрийн хос эсвэл өөрчлөлт хийх аль аль үед чухал хэрэгцээтэй байдаг.

Хамаарах ГОБ түлхүүрийг адилтгагчийн аргыг заавал хэрэглэх ёстой бөгөөд олгож буй бүх ХГЖ-ууддаа энэ өргөтгөлийг заавал оруулна.

5.2.2 Гэрчилгээ олгогчийн нэмэлт нэр

Гэрчилгээ олгогчийн нэмэлт нэр гэсэн өргөтгөл нь тухайн ХГЖ-ын олгогчтой холбоотой нэмэлт адилтгал (танилт) юм. Электрон мэйл хаяг (rfc822Name), DNS хаяг, IP хаяг болон URI гэсэн сонголтууд байдаг. Нэг болон олон нэрийг оруулах талбартай. Энэ төрлийн адилтгалуудыг хэдий ч хэрэглэсэн гэрчилгээ олгогчийн нэмэлт нэрийн өргөтгөл хэрэглэгдэнэ. Гэхдээ DNS нэрийг хэсэг 4.1.2.4-д тайлбарласан domainComponent шинж чанарыг хэрэглэн харуулж болно.

Хамаарах ГОБ issurAltName өргөтгөлийг чухал биш гэж тэмдэглэнэ.

5.2.3. ХГЖ-ын дугаар

ХГЖ-ын дугаар нь ХГЖ-ын хамрах хүрээ болон ХГЖ-ын олгогчийн нэг хэвийн байдлаар өсдөг дарааллын дугаарыг дүрсэлдэг чухал биш ХГЖ-ын өргөтгөл юм. Тухайн ХГЖ нь өөр ХГЖ-ыг цуцлахыг энэ өргөтгөлөөр хэрэглэгчид хялбар тодорхойлох боломжтой. ХГЖ-ын дугааараар бүрэн ХГЖ болон дельта ХГЖ-уудыг адилтган танина. Энэ профайлыг хамаарах ГОБ-ын ХГЖ-ууддаа энэ өргөтгөлийг оруулах ёстой бөгөөд чухал биш гэж тэмдэглэнэ.

Аливаа ХГЖ олгогч нь тухайн хамрах хүрээнд бүрэн ХГЖ дээр нэмээд дельта ХГЖ-ыг үүсгэвэл тухайн бүрэн болон дельта ХГЖ-ууд нэг дарааллын дугаарыг дундаа хэрэглэнэ. Нэг ижил хамрах хүрээний дельта ХГЖ болон бүрэн ХГЖ-ыг тухайн агшинд зэрэг олговол ХГЖ-ууд нь ижил ХГЖ-ын дугаартай байх ёстой бөгөөд хүчингүй гэрчилгээнүүдийн мэдээлэл нь ижил байна. Энэ нь тухайн дельта ХГЖ болон аливаа хүлээн зөвшөөрөгдөхүйц бүрэн ХГЖ-ын нэгдэл нь зэрэг олгогдсон бүрэн ХГЖ шиг ижил хүчингүй болгосон мэдээллээр хангана.

Аливаа ХГЖ-ыг олгогч нь хоёр ширхэг ХГЖ (хоёр бүрэн ХГЖ, хоёр дельта ХГЖ эсвэл нэг бүрэн ХГЖ болон нэг дельта ХГЖ) ялгаатай хугацааны агшинд ижил хамрах хүрээнд үүсгэвэл тухайн хоёр ХГЖ нь ижил ХГЖ-ын дугаартай байх ёсгүй. Энэ нь тухайн хоёр ХГЖ-ын энэ талбар (Хэсэг 5.1.2.4) нь ижил биш байвал ХГЖ-ын дугаарууд ялгаатай байх ёстой.

Дээрх шаардлагын дагуу ХГЖ-ын дугаарууд нь Long бүхэл тоогоор илэрхийлэгдэх боломжтой. Хамаарах ГОБ-аас CRLNumber утга нь 20 октетоос ихгүй байх ёстой.

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }
  CRLNumber ::= INTEGER (0..MAX)
```

5.2.4. Дельта ХГЖ-ын үзүүлэлт

Дельта ХГЖ-ын үзүүлэлт нь ХГЖ-ын чухал өргөтгөл бөгөөд дельта ХГЖ гэж адилтган танигдана. Дельта ХГЖ нь бүрэн ХГЖ-нд дүрслэгддэг бүх мэдээллээс гадна урьдчилан тараагдсан хүчингүй гэрчилгээнүүдийн мэдээллийн шинэчлэлийг агуулдаг. Дельта ХГЖ-ыг хэрэглэх нь зарим орчинд сүлжээний ачаалал, боловсруулах хугацааг огцом бууруулдаг. Дельта ХГЖ нь шинэчилж буй ХГЖ-аасаа ерөнхийдөө бага хэмжээтэй байдаг. Тиймээс дельта ХГЖ-ыг хүлээн авдаг аппликейшнүүд бүрэн ХГЖ-ыг хүлээж авдаг аппликейшнүүдтэй харьцуулахад сүлжээний зурвасыг бага хэрэглэдэг. ХГЖ-ын бүтцээс ялгаатай форматаар хүчингүй гэрчилгээнүүдийн мэдээллийг хадгалдаг аппликейшнүүд дахин боловсруулалт хийхгүйгээр шинэ хүчингүй гэрчилгээнүүдийн

мэдээллүүдийг нэмдэг.

Дельта ХГЖ-ын үзүүлэлт өргөтгөл нь BaseCRLNumber төрлийн цор ганц утгыг агуулдаг. Энэ ХГЖ-ын дугаараар аливаа хамрах хүрээн дэх бүрэн ХГЖ-ыг танина. Энэ нь дельта ХГЖ-ыг үүсгэх эхлэлийн цэг болдог. Хамаарах ГОБ нь бүрэн ХГЖ шиг иш татсан үндсэн ХГЖ-уудыг харуулах ёстой. Тухайн дельта ХГЖ нь тухайн ижил хамрах хүрээний хүчингүй төлөвүүдийн бүх шинэчлэлүүдийг агуулдаг. Дельта ХГЖ дээр иш татсан үндсэн ХГЖ-уудыг нэмсэн нэгтгэл нь тухайн дельта ХГЖ-уудын зарлагдаж буй хугацаанд хэрэгжиж буй хамрах хүрээний бүрэн ХГЖ-тай ижил юм.

Хамаарах аливаа ГОБ нь үүсгэсэн дельта ХГЖ-нд чухал дельта ХГЖ-ын үзүүлэлт гэсэн өргөтгөлийг оруулах ёстой.

Аливаа дельта ХГЖ-ыг олгохдоо түүний иш татсан үндсэн ХГЖ-уудыг агуулсан шалтгаанууд болон гэрчилгээнүүдийг бүгдийг багтаадаг. Энэ нь, тухайн дельта ХГЖ-ын хамрах хүрээ нь иш татсан үндсэн бүрэн ХГЖ-ын хамрах хүрээтэй ижил байх ёстой. Тухайн иш татсан үндсэн ХГЖ болон дельта ХГЖ нь гэрчилгээ олгодог түгээх цэгийн өргөтгөлийг орхих эсвэл адилтгах түгээх цэгийн өргөтгөлүүдийг агуулна. Цаашид ХГЖ-ын олгогч нь тухайн дельта ХГЖ болон түүгээр шинэчлэгдэж буй аливаа бүрэн ХГЖ-уудад гарын үсэг зурахдаа ижил хувийн түлхүүр хэрэглэх ёстой.

Дельта ХГЖ-уудыг дэмжиж ажилладаг аппликешн нь тухайн хамрах хүрээнд бүрэн олгогдсон аливаа ХГЖ эсвэл тухайн хамрах хүрээнд бүрэн дотооддоо бүрдүүлсэн ХГЖ-ын аль нэгээр тухайн хамрах хүрээний аливаа дельта ХГЖ-тай нэгтгэж бүрэн ХГЖ-ыг бүрдүүлдэг.

Аливаа дельта ХГЖ-ыг аливаа бүрэн эсвэл дотооддоо бүрдүүлсэн ХГЖ-тай нэгтгэхэд дотоодоо бүрдүүлсэн ХГЖ нь бүрдүүлэлтэд хэрэглэгдсэн дельта ХГЖ-ын ХГЖ дугаар өргөтгөлд тодорхойлогдсон дугаартай байна. Нэмж хэлэхэд дотоодоо бүрдүүлсэн ХГЖ нь бүрдүүлэлтэд хэрэглэгдсэн дельта ХГЖ-ын хамаарах өргөтгөлүүдэд тодорхойлогдсон thisUpdate болон nextUpdate-тай байна. Нэмэлтээр, дотооддоо бүрдүүлсэн ХГЖ нь бүрдүүлэлтэд хэрэглэгдсэн дельта ХГЖ-ыг олгож буй түгээлтийн цэгээс уламжлагдаж гардаг.

Аливаа бүрэн ХГЖ болон дельта ХГЖ-ыг дараах дөрвөн нөхцөл биелэгдсэн тохиолдолд нэгтгэх боломжтой. Үүнд:

A) Тухайн бүрэн ХГЖ болон тухайн дельта ХГЖ нь нэг ижил олгогчтой байх.

B) Тухайн бүрэн ХГЖ блон тухайн дельта ХГЖ нь нэг хамрах хүрээтэй байх. Аль аль нь доорх хоёр нөхцөлийн аль нэгийг хангаж байвал ижил хамрах

хүрээтэй гэж үзнэ. Үүнд:

1) issuingDistributionPoint өргөтгөл тухайн бүрэн ХГЖ болон тухайн ХГЖ-ын аль алинаас нь хасагдсан байх

2) issuingDistributionPoint өргөтгөл тухайн бүрэн ХГЖ болон тухайн дельта ХГЖ-ын аль алиных нь хувьд байвал бүх талбаруудын утгууд нь ижил байх

C) Тухайн бүрэн ХГЖ-ын ХГЖ дугаар нь тухайн дельта ХГЖ-д тодорхойлогдсон BaseCRLNumber тай тэнцүү эсвэл их байх. Энэ нь, тухайн бүрэн ХГЖ нь (хамгийн багадаа) иш татсан үндсэн ХГЖ-уудын бүх хүчин гэрчилгээнүүдийн мэдээллийг агуулдаг.

D) Тухайн бүрэн ХГЖ-ын ХГЖ дугаар нь тухайн дельта ХГЖ-ын ХГЖ дугаараас бага байх. Энэ нь, тухайн дельта ХГЖ нь дараалллын дугаарааараа бүрэн ХГЖ-ыг дагана.

ХГЖ-ыг олгогчид дельта ХГЖ болон зохих бүрэн ХГЖ-ын хослол нь одоогийн хүчингүй болгох статусыг үнэн зөв тусгаж буйг нягтлах ёстой. ХГЖ-ыг олгогч нь иш татсан үндсэн ХГЖ-ыг үүсгэснээс хойш статус нь өөрчлөгдсөн дельта ХГЖ-ын хамрах хүрээний гэрчилгээ бүрийн хувьд дельта ХГЖ-д бичилт оруулах ёстой.

A) Хэрэв ХГЖ-д багтсан шалтгаанаар гэрчилгээг хүчингүй болгосон бол гэрчилгээг хүчингүй болсон гэж бичнэ.

B) Хэрэв тухайн гэрчилгээ нь хүчинтэй бөгөөд иш татсан үндсэн ХГЖ эсвэл CertificateHold шалтгааны код бүхий дараагийн ХГЖ-д жагсаагдсан бол CertificateHold шалтгааны кодыг removeFromCRL шалтгааны кодтой гэрчилгээний жагсаалтад оруулна.

C) Хэрэв гэрчилгээ нь ХГЖ-ын хамрах хүрээнээс гадуурх шалтгаанаар хүчингүй болсон боловч гэрчилгээ нь иш татсан үндсэн ХГЖ эсвэл ХГЖ-ын хамрах хүрээнд орсон шалтгааны код бүхий дараагийн ХГЖ-д бичигдсэн бол гэрчилгээг хүчингүй болгоно гэхдээ шалтгааны кодыг орхино.

D) Хэрэв гэрчилгээ нь ХГЖ-ын хамрах хүрээнээс өөр шалтгаанаар хүчингүй болсон бөгөөд гэрчилгээ нь иш татсан үндсэн ХГЖ болон энэ ХГЖ-ын хамрах хүрээнд орсон шалтгааны кодтой дараагийн ХГЖ-д ороогүй бол гэрчилгээг энэ ХГЖ-д оруулахгүй.

Гэрчилгээ хүчингүй болсон тохиолдолд (certificateHold гэх мэт хүчингүй болгох шалтгаанаар), хүлээлтээс чөлөөлөгдсөн эсвэл хүчингүй болгох шалтгаан өөрчлөгдсөн тохиолдолд гэрчилгээний статус өөрчлөгдсөн гэж үзнэ.

Иш татсан үндсэн ХГЖ-д гэрчилгээг оруулаагүй байсан ч removeFromCRL шалтгааны кодтой бол дельта ХГЖ-нд оруулах нь зүйтэй. Хэрэв гэрчилгээ нь үндсэн ХГЖ-ны дараа гэхдээ энэ дельта ХГЖ-аас өмнө гарсан аливаа ХГЖ-нд хүлээлтэд ороод, дараа нь хүлээлтээс чөлөөлөгдсөн бол түүнийг removeFromCRL цуцлах шалтгааны хамт дельта ХГЖ дээр ЗААВАЛ бичиж оруулна.

Хэрэв гэрчилгээнд заасан notAfter хугацаа нь дельта ХГЖ- д заасан thisUpdate хугацаанаас өмнө байгаа бөгөөд гэрчилгээ нь иш татсан үндсэн ХГЖ-д орсон байсан эсвэл иш татсан үндсэн ХГЖ-ын дараа олгосон ХГЖ-д орсон гэхдээ энэ нь дельта ХГЖ-ээс өмнө байвал ХГЖ олгогч нь дельта ХГЖ дээр гэрчилгээг removeFromCRL шалтгаан кодоор бичиж оруулж болно.

Хэрэв гэрчилгээг хүчингүй болгох мэдэгдэл эхлээд дельта ХГЖ дээр гарч ирвэл ижил хамрах хүрээний дараагийн бүрэн ХГЖ гарахаас өмнө гэрчилгээний хүчинтэй байх хугацааг дуусах боломжтой. Энэ тохиолдолд хүчингүй болгох мэдэгдлийг дор хаяж нэг тодорхой гаргасан иж бүрэн ХГЖ-д хүчингүй болгох мэдэгдлийг оруулах хүртэл дараагийн бүх дельта ХГЖ-д ЗААВАЛ оруулах ёстой.

Дельта ХГЖ-ыг дэмждэг аппликейшн нь өмнө нь гаргасан бүрэн ХГЖ болон хамгийн сүүлийн үеийн дельта ХГЖ-ыг нэгтгэж одоогийн бүрэн ХГЖ-ыг ЗААВАЛ үүсгэнэ. Дельта ХГЖ-ыг дэмждэг программ нь өмнө нь дотооддоо гарсан бүрэн ХГЖ болон одоогийн дельта ХГЖ-ыг нэгтгэснээр одоогийн бүрэн ХГЖ-ийг үүсгэх боломжтой. Хэрэв одоогийн цаг нь thisUpdate болон nextUpdate талбарт байгаа цагуудын хооронд байвал дельта ХГЖ-ыг одоогийнх гэж үзнэ. Зарим тохиолдолд ХГЖ олгогч нь nextUpdate талбарт заасан хугацаанаас өмнө нэг буюу хэд хэдэн дельта ХГЖ-ыг гаргаж болно. Өгөгдсөн хамрах хүрээний нэгээс олон одоогийн дельта ХГЖ-тай тулгарвал аппликейшн нь thisUpdate-д хамгийн сүүлийн үеийн утгыг хамгийн сүүлийн үеийнх гэж үзнэ.

id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= { id-ce 27 }

BaseCRLNumber ::= CRLNumber

5.2.5.2 Олголтын түгээлтийн цэг (ОТЦ)

ОТЦ нь ХГЖ-ыг түгээлтийн цэгийг болон тодорхой ХГЖ-ын хамрах хүрээг тодорхойлдог чухал ХГЖ өргөтгөл бөгөөд энэ нь ХГЖ нь зөвхөн эцсийн байгууллагын хүчингүй гэрчилгээ, зөвхөн ГОБ-ын гэрчилгээ, зөвхөн шинж

чанаруудын гэрчилгээ эсвэл хязгаарлагдмал шалтгааны кодуудын хүчингүй мэдээллийг хамрах эсэхийг заадаг. Хэдийгээр өргөтгөл нь чухал боловч хамаарах хэрэгжүүлэлтүүд нь энэ өргөтгөлийг дэмжсэн байхыг шаарддаггүй. Гэсэн хэдий ч, энэ өргөтгөлийг дэмждэггүй хэрэгжүүлэлтүүд нь ХГЖ дээр бичигдээгүй аливаа гэрчилгээний статусыг тодорхойгүй гэж үзэх эсвэл танигдаагүй чухал өргөтгөлүүдийг агуулаагүй өөр ХГЖ-ыг олох ЗААВАЛ хэрэгтэй.

ХГЖ олгогч нь өөрийн хувийн түлхүүрээр ХГЖ-д гарын үсэг зурна. ХГЖ түгээлтийн цэгүүдэд өөрийн гэсэн хос түлхүүр байдаггүй. Хэрэв ХГЖ нь X.500 директорт хадгалагдсан бол ХГЖ түгээгчийн директорт хадгалагдана. Энэ директор нь ХГЖ олгогчийн мэдээллээс ялгаатай байна.

Түгээлтийн цэгтэй холбоотой шалтгааны кодуудыг onlySomeReasons-д зааж өгөх ёстой. Хэрэв onlySomeReasons гарч ирэхгүй бол түгээлтийн цэг нь бүх шалтгааны кодыг хүчингүй болгох ёстой. ГОБ-ууд түр болон байнгын хүчингүй болгох үндсэн дээр ХГЖ-ыг хуваахдаа ХГЖ түгээлтийн цэгүүдийг ашиглаж болно. Энэ тохиолдолд keyCompromise (1), cACompromise (2), aACompromise (8) шалтгаан кодтой хүчингүй болгох нь нэг түгээлтийн цэгт, бусад шалтгааны код бүхий хүчингүй болгох нь өөр түгээлтийн цэг дээр гарч ирнэ.

Хэрэв ХГЖ-д onlySomeReasons-тай issuingDistributionPoint өргөтгөл байгаа бол байгаа бол хүчингүй болсон ХГЖ-ын хамрах хүрээний гэрчилгээ бүрд тодорхойгүйгээс өөр хүчингүй болгох шалтгаан ЗААВАЛ оноох ёстой. Хүчингүй болсон гэрчилгээг аль ХГЖ(ууд) дээр жагсаахыг тодорхойлоход өгөгдсөн хүчингүй болгох шалтгааныг ашигладаг боловч харгалзах ХГЖ бичилтэд reasonCode ХГЖ бичилтийн өргөтгөлийг оруулах шаардлагагүй.

DistributionPoint талбарын синтакс болон семантик нь cRLDistributionPoints өргөтгөл дэх distributionPoint талбартай ижил байна (Хэсэг 4.2.1.13). Хэрэв түгээлтийн цэг байгаа бол энэ нь ХГЖ-ын хамрах хүрээний гэрчилгээ бүрийн cRLDistributionPoints өргөтгөлийн хамаарах distributionPoint талбараас багадаа нэгээс доошгүй нэрийг ЗААВАЛ оруулна. Ижил кодчиллыг гэрчилгээ болон ХГЖ-ын түгээлтийн цэгийн талбарт ЗААВАЛ ашиглах ёстой.

Хэрэв түгээлтийн цэгийн талбар байхгүй бол ХГЖ-д ХГЖ-ын хамрах хүрээн дэх ХГЖ олгогчоос олгосон дууссан болсон хүчингүй болсон бүх гэрчилгээний бичилтүүд байх ёстой.

Хэрэв ХГЖ-ын хамрах хүрээ нь зөвхөн ХГЖ олгогчоос олгосон гэрчилгээг багтаасан бол indirectCRL boolean утгыг ХУДАЛ гэж тохируулсан байх ёстой. Үгүй бол, хэрэв ХГЖ-ын хамрах хүрээ нь ХГЖ олгогчоос өөр нэг буюу хэд хэдэн

эрх бүхий байгууллагаас олгосон гэрчилгээг багтаасан бол indirectCRL boolean утгыг ҮНЭН гэж тохируулах ёстой. Бичлэг бүрийг хариуцах эрх бүхий байгууллагыг гэрчилгээ олгогчийн ХГЖ бичилтийн өргөтгөлөөр зааж өгнө(Хэсэг 5.3.3).

Хэрэв ХГЖ-ын хамрах хүрээ нь зөвхөн эцсийн нэгжийн нийтийн түлхүүрийн гэрчилгээг агуулж байвал зөвхөн ContainsUserCerts-ийг ҮНЭН гэж ЗААВАЛ тохируулах хэрэгтэй. Хэрэв ХГЖ-ын хамрах хүрээ нь зөвхөн ГОБ-ын гэрчилгээг агуулж байвал зөвхөн ContainsCACerts-г ҮНЭН гэж тохируулсан байх ёстой. Хэрэв onlyContainsUserCerts эсвэл onlyContainsCACerts-ийн аль нэгийг нь ҮНЭН гэж тохируулсан бол ХГЖ-ын хамрах хүрээ нь 1 эсвэл 2-р хувилбарын гэрчилгээг ОРУУЛАХ ЁСТОЙ. Хамаарах ХГЖ олгогчид onlyContainsAttributeCerts логикийг ХУДАЛ болгож ЗААВАЛ тохируулна.

Хамаарах ХГЖ олгогчид олгох түгээлтийн цэгийн өргөтгөлийн DER кодчилол нь хоосон дараалалтай байвал ХГЖ-ыг гаргаж болохгүй. Өөрөөр хэлбэл, onlyContainsUserCerts, onlyContainsCACerts indirectCRL, onlyContainsAttributeCerts нь бүгд ХУДАЛ байвал, түгээлтийнPoint талбар эсвэл onlySomeReasons талбар ЗААВАЛ байх ёстой.

```
id-ce-issuingDistributionPoint OBJECT IDENTIFIER  ::= { id-ce 28 }
IssuingDistributionPoint ::= SEQUENCE {
distributionPoint
onlyContainsUserCerts
onlyContainsCACerts
onlySomeReasons
indirectCRL
onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE }
[0] DistributionPointName OPTIONAL,
[1] BOOLEAN DEFAULT FALSE,
[2] BOOLEAN DEFAULT FALSE,
[3] ReasonFlags OPTIONAL,
[4] BOOLEAN DEFAULT FALSE,
    - - at most one of onlyContainsUserCerts, onlyContainsCACerts,
    - - and onlyContainsAttributeCerts may be set to TRUE.
```

5.2.6. Хамгийн шинэ ХГЖ (a.k.a. дельта ХГЖ түгээх цэг)

Хамгийн шинэ ХГЖ өргөтгөл нь бүрэн ХГЖ-ын дельта ХГЖ мэдээллийг хэрхэн олж авахыг тодорхойлдог. Хамаарах ХГЖ олгогчид энэ өргөтгөлийг чухал биш гэж ЗААВАЛ тэмдэглэнэ. Энэ өргөтгөл нь дельта ХГЖ-д ЗААВАЛ дүрслэгдэх албагүй.

Энэ өргөтгөлд cRLDistributionPoints гэрчилгээний өргөтгөлтэй ижил синтаксийг ашигласан бөгөөд 4.2.1.13-т тайлбарласан болно. Гэсэн хэдий ч зөвхөн түгээлтийн цэгийн талбар нь энэ нөхцөлд утга учиртай юм. Шалтгаан болон cRLIssuer талбаруудыг энэ ХГЖ өргөтгөлөөс хассан байх ёстой.

Түгээх цэгийн нэр бүр нь энэ бүрэн ХГЖ-ын дельта ХГЖ-ыг олж болох байршлыг өгдөг. Эдгээр дельта ХГЖ-ын хамрах хүрээ нь энэхүү бүрэн ХГЖ-ын хамрах хүрээтэй ижил байх ёстой. Энэ ХГЖ өргөтгөлийн агуулгыг зөвхөн дельта ХГЖ-ыг олоход ашигладаг; Агуулга нь ХГЖ эсвэл иш татсан дельта ХГЖ-ыг баталгаажуулахад ашиглагддаггүй. 4.2.1.13-д заасан түгээлтийн цэгүүдэд тодорхойлсон кодчилол нь энэ өргөтгөлд хамаарна.

```
id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ce 46 }
  FreshestCRL ::= CRLDistributionPoints
```

5.2.7. Эрх бүхий байгууллагын мэдээллийн хандалт

Энэ хэсэгт ХГЖ-д эрх бүхий байгууллагын мэдээллийн хандалт өргөтгөлийн хэрэглээг авч үзнэ. Гэрчилгээний өргөтгөлийн 4.2.2.1-д тодорхойлсон синтакс болон семантикийг ХГЖ-ын өргөтгөлд мөн ашигладаг.

Энэхүү ХГЖ-ын өргөтгөл нь чухал биш гэж тэмдэглэгдсэн байх ёстой.

ХГЖ-д байгаа тохиолдолд энэ өргөтгөл нь id-ad-caIssuers-ийг accessMethod болгон зааж өгсөн ядаж нэг AccessDescription-г агуулсан байх ёстой. id-ad-caIssuers OA нь ХГЖ дээрх гарын үсгийг баталгаажуулахад ашиглагдах гэрчилгээг жагсаахад хэрэглэгдэнэ (жишээ нь ХГЖ дээрх олгогчийн нэртэй таарч байгаа субъектийн нэртэй, ХГЖ дээр гарын үсэг зурахад хэрэглэсэн хувийн түлхүүрт хамаарах субъектийн нийтийн түлхүүртэй). id-ad-caIssuers-аас бусад хандалтын аргын төрлүүд нь ЗААВАЛ орохгүй. AccessDescription-ийн дор хаяж нэг тохиолдол нь HTTP [RFC2616] эсвэл LDAP [RFC4516] URI болох accessLocation-ийг заах ХЭРЭГТЭЙ.

Мэдээллийг HTTP эсвэл FTP-ээр авах боломжтой тохиолдолд accessLocation нь нэг төрлийн нөөцийн танигч байх ёстой бөгөөд URI нь [RFC2585]-д заасны дагуу гэрчилгээг кодолсон цор ганц DER эсвэл [RFC2797]-д заасны дагуу "зөвхөн гэрчилгээ" CMS мессежээр кодолсон BER эсвэл DER-ийн гэрчилгээний цуглуулгыг зааж өгөх ёстой.

Гэрчилгээнүүд рүү хандахын тулд HTTP эсвэл FTP-г дэмждэг хамаарах аппликейшнууд нь гэрчилгээг кодолсон бие даасан DER-ийг хүлээн авах

ЁСТОЙ бөгөөд "зөвхөн гэрчилгээ" CMS мессежийг хүлээн авах боломжтой байх ХЭРЭГТЭЙ.

URI-ээр дамжуулан хандсан HTTP серверийн хандалтууд нь хариултын агуулгын-төрөл толгой талбарт медиа төрлийн аппликейшн/pkix- гэрчилгээг [RFC2585] зааж өгөх ХЭРЭГТЭЙ бөгөөд "зөвхөн гэрчилгээ" CMS мессежний хариултын агуулгын төрлийн толгой хэсэгт медиа төрлийн аппликейшн/pkcs7-mime [RFC2797]-г зааж өгөх ЁСТОЙ. FTP-ийн хувьд гэрчилгээг кодолсон цор ганц DER-ын агуулсан файлын нэрэнд ".cer" [RFC2585] дагавар байх ЁСТОЙ, "зөвхөн гэрчилгээ" CMS мессеж агуулсан файлын нэр нь "p7c" [RFC2797] дагавартай БАЙХ ХЭРЭГТЭЙ. Хамаарах үйлчлүүлэгчид медиа төрөл эсвэл файлын өргөтгөлийг контентын сануулга болгон ашиглаж болох боловч серверийн хариу үйлдэлд зөвхөн зөв медиа төрөл эсвэл файлын өргөтгөл байгаа эсэхээс хамаарахгүй.

AccessLocation нь директорийн нэр байх үед директор серверийг дотооддоо тохируулсан байгаа хаанаас ч аппликейшнээр мэдээллийг авна. Гэрчилгээ болон ХГЖ дээрх гарын үсгийг баталгаажуулахын тулд нэг ГОБ-ын нийтийн түлхүүрийг хэрэглэх үед хүссэн ГОБ-ын гэрчилгээ нь [RFC4523]-д заасны дагуу crossCertificatePair ба/эсвэл cACertificate шинж чанаруудад хадгалагдана. Гэрчилгээ болон ХГЖ дээрх гарын үсгийг баталгаажуулахын тулд өөр нийтийн түлхүүрийг ашиглах үед хүссэн гэрчилгээ нь [RFC4523]-д заасан userCertificate шинж чанарт хадгалагдана. Иймд accessLocation-ийн директорын нэрийн хэлбэрийг дэмждэг хэрэгжүүлэлтүүд нь эдгээр гурван шинж чанарын аль нэгэнд шаардлагатай гэрчилгээг олоход бэлтгэгдсэн байх ЁСТОЙ. Аппликейшн нь директор руу хандахын тулд ашигладаг протокол (жишээ нь, DAP эсвэл LDAP) нь дотоод байна.

Мэдээллийг LDAP-аар авах боломжтой тохиолдолд accessLocation нь uniformResourceIdentifier байх ХЭРЭГТЭЙ. LDAP URI [RFC4516] нь гэрчилгээг эзэмшиж буй оруулгын ялгагдах нэрийг агуулсан <dn> талбарыг ЗААВАЛ оруулах ёстой бөгөөд гэрчилгээг кодолсон DER гэрчилгээнүүд эсвэл кросс гэрчилгээний хослол [RFC4523]-ыг агуулсан шинж чанаруудын тохирох шинж чанарын тайлбарыг жагсаасан <attributes> талбарыг ЗААВАЛ оруулах ёстой, мөн <host> (жишээ нь: <ldap://ldap.example.com/cn=CA, dc=example,dc=com?cACertificate;binary,crossCertificatePair;binary>)-ыг оруулах ХЭРЭГТЭЙ. <host> (жишээ нь: <ldap:///cn=exampleCA,dc=example,dc=com?cACertificate;binary>)-г орхих нь үйлчлүүлэгч зохих сервертэй холбогдохын тулд ямар ч зэрэглэлийн мэдлэгт найдах нөлөөтэй.

5.3. ХГЖ бичилтийн өргөтгөлүүд

X.509-ын хувилбар 2 ХГЖ-д зориулсан ISO/IEC, ITU-T болон ANSI X9 нийгэмлэгүүдийн тодорхойлсон ХГЖ бичилтийн өргөтгөлүүд нь [X.509] [X9.55] ХГЖ бичилтүүдтэй нэмэлт шинж чанаруудыг холбох аргуудаар хангадаг. X.509-ын хувилбар 2 ХГЖ формат нь тухайн нийгэмлэг рүү мэдээллийг цор ганц дамжуулахын тулд хувийн ХГЖ бичилтийн өргөтгөлүүдийг тодорхойлох боломжийг нийгэмлэгүүдэд олгодог. ХГЖ бичилтийн өргөтгөл бүрийг чухал эсвэл чухал биш гэж тодорхойлж болно. Хэрэв ХГЖ нь аппликейшн боловсруулах боломжгүй ХГЖ бичилтийн чухал өргөтгөлтэй бол тухайн аппликейшн нь тухайн ХГЖ-г гэрчилгээний статусыг тодорхойлохын тулд ашиглах ёсгүй. Гэсэн хэдий ч, аппликейшнүүд нь хүлээн зөвшөөрөгдөөгүй ХГЖ бичилтийн өргөтгөлүүдийг алгасаж болно.

Дараах дэд хэсгүүдэд Интернэт ХГЖ бичилтүүд болон мэдээллийн стандарт байршлуудад ашиглагдах санал болгож буй өргөтгөлүүдийг үзүүлнэ. Нийгэмлэгүүд ХГЖ бичилтэд нэмэлт өргөтгөлүүдийг ашиглахаар сонгож болно; Гэсэн хэдий ч ерөнхий контекстэд ашиглаж болох ХГЖ-д ХГЖ бичилтийн чухал өргөтгөлүүдийг ашиглахдаа анхааралтай хандах хэрэгтэй.

Энэ тодорхойлолтод оруулсан ХГЖ бичилтийн өргөтгөлүүдийн дэмжлэг нь ХГЖ олгогчид болон аппликейнүүдэд тохирох сонголт юм. Гэсэн хэдий ч ХГЖ олгогчид нь энэ мэдээлэл байгаа үед шалтгааны код (5.3.1-р хэсэг) болон хүчингүй болсон огноо (5.3.2-р хэсэг)-ийг оруулах ХЭРЭГТЭЙ.

5.3.1. Шалтгааны код

reasonCode нь гэрчилгээг хүчингүй болгох шалтгааныг тодорхойлсон чухал биш ХГЖ бичилтийн өргөтгөл юм. ХГЖ олгогчдод ХГЖ бичилтэд утга учиртай шалтгааны код оруулахыг зөвлөдөг; гэхдээ тодорхойгүй (0) reasonCode утгыг ашиглахын оронд шалтгааны кодын ХГЖ бичилтийн өргөтгөл байхгүй байх ХЭРЭГТЭЙ.

RemoveFromCRL (8) reasonCode утга нь зөвхөн дельта ХГЖ-д гарч ирэх бөгөөд гэрчилгээний хугацаа дууссан эсвэл хүлээлтээс хасагдсан тул гэрчилгээг ХГЖ-аас устгах ёстойг илтгэнэ. Бусад бүх шалтгааны кодууд нь дурын ХГЖ-д гарч ирэх бөгөөд заасан гэрчилгээг хүчингүй болсонд тооцох ёстойг харуулж байна.

```
id-ce-cRLReasons OBJECT IDENTIFIER  ::= { id-ce 21 }
-- reasonCode ::= { CRLReason }
CRLReason ::= ENUMERATED {
    unspecified                     (0),
```

```
    keyCompromise                  (1),
    cACompromise                   (2),
    affiliationChanged             (3),
    superseded                     (4),
    cessationOfOperation           (5),
    certificateHold                (6),
       - - value 7 is not used
    removeFromCRL                  (8),
    privilegeWithdrawn             (9),
    aACompromise                  (10) }
```

5.3.2. Хүчингүй болгосон огноо

Хүчингүй болсон огноо нь хувийн түлхүүр алдагдсан эсвэл гэрчилгээ нь хүчингүй болсон нь мэдэгдэж байгаа эсвэл сэжиглэгдсэн огноог агуулсан чухал биш ХГЖ бичилтийн өргөтгөл юм. Энэ огноо нь ХГЖ-ын бичилт дэх хүчингүй болсон өдрөөс өмнө байж болох бөгөөд энэ нь ГОБ нь хүчингүй болгох үйлдлийг хийсэн огноо юм. Хүчингүй болгох тухай ХГЖ олгогч нь эхэлж ХГЖ-д нийтлэх үед баталгаагүй болсон огноо нь өмнөх ХГЖ-уудыг гаргасан огнооноос өмнө байж болох ч хүчингүй болсон огноо нь өмнөх ХГЖ-уудыг гаргасан огнооноос өмнө байж болохгүй. Энэ мэдээллийг хэзээд ХГЖ олгогчид нь ХГЖ хэрэглэгчдэдээ мэдээлэх зайлшгүй хэрэгтэй.

Энэ талбарт орсон GeneralizedTime утгуудыг ЗААВАЛ Гринвичийн дундаж цагаар (Зулу) илэрхийлэх ба 4.1.2.5.2-т заасанчлан зааж, тайлбарлах ёстой.

```
id-ce-invalidityDate OBJECT IDENTIFIER  ::= { id-ce 24 }
  InvalidityDate ::=  GeneralizedTime
```

5.3.3. Гэрчилгээ олгогч

Энэхүү ХГЖ бичилтийн өргөтгөл нь шууд бус ХГЖ-ын бичилттэй холбоотой гэрчилгээ олгогчийг тодорхойлдог, өөрөөр хэлбэл түгээлтийн цэгийн өргөтгөлдөө indirectCRL үзүүлэлтийг тохируулсан ХГЖ юм. Байгаа тохиолдолд гэрчилгээ олгогчийн ХГЖ бичилтийн өргөтгөл нь олгогчийн талбар ба/эсвэл ХГЖ бичилттэй хамаарах гэрчилгээ олгогчийн өөр нэрийн өргөтгөлөөс нэг буюу хэд хэдэн нэр агуулна. Хэрэв энэ өргөтгөл нь шууд бус ХГЖ-ын эхний бичилтэд байхгүй бол гэрчилгээ олгогч нь ХГЖ олгогчийг анхдагч болгож өгдөг. Шууд бус ХГЖ-ын дараагийн бичилтүүд дээр, хэрэв энэ өргөтгөл байхгүй бол уг бичилтийн гэрчилгээ олгогч нь өмнөх бичилтийнхтэй ижил байна. Энэ талбарыг дараах байдлаар тодорхойлно.

```
  id-ce-certificateIssuer   OBJECT IDENTIFIER  ::= { id-ce 29 }
```

```
CertificateIssuer ::=     GeneralNames
```

Хамаарах ХГЖ олгогчид энэхүү өргөтгөлд ХГЖ-ийн бичилтэд тохирох гэрчилгээ олгогчийн талбараас ЯН-ийг ЗААВАЛ оруулна. ЯН-ийн кодчилол нь гэрчилгээнд ашигласан кодчилолтой ижил байх ёстой.

ХГЖ олгогчид энэ өргөтгөлийг ЗААВАЛ чухал гэж тэмдэглэснээр энэ өргөтгөлийг орхигдуулбал ХГЖ бичилтүүдийг гэрчилгээнд зөв хамааруулах боломжгүй. Энэхүү тодорхойлолт нь энэ өргөтгөлийг хэрэгжүүлэлтүүд нь таньдаг байхыг ЗӨВЛӨЖ БАЙНА.

6. Гэрчилгээжүүлэлтийн замын баталгаажуулалт

Интернэт НТДБ-д зориулсан гэрчилгээжүүлэлтийн замын баталгаажуулалтын процедур нь [X.509]-д өгөгдсөн алгоритм дээр суурилдаг. Гэрчилгээжүүлэх замын боловсруулалт нь субъектийн ялгагдах нэр ба/эсвэл субъектийн өөр нэр болон субъектийн нийтийн түлхүүрийн хоорондын уялдаа холбоог баталгаажуулдаг. Уялдаа холбоо нь итгэмжлэгдсэн талын заасан зам, оролтыг агуулсан гэрчилгээнд заасан хязгаарлалтаар хязгаарлагддаг. Үндсэн хязгаарлалтууд болон бодлогын хязгаарлалтуудын өргөтгөлүүд нь шийдвэр гаргах үйл явцыг автоматжуулахын тулд гэрчилгээжүүлэлтийн замыг боловсруулалтын логикийг боломжтой болгодог.

Энэ хэсэгт гэрчилгээжүүлэлтийн замыг баталгаажуулах алгоритмыг тайлбарласан болно. Энэ алгоритмыг хэрэгжүүлэхийн тулд энэхүү тодорхойлолтод нийцсэн хэрэгжилтийг хийх шаардлагагүй, гэхдээ энэ процедурын үр дүнд бий болсон гадаад шинжтэй дүйцэхүйц үйл ажиллагааг хангах ёстой. Аливаа алгоритмыг зөв үр дүнд хүрсэн тохиолдолд тодорхой хэрэгжүүлэлт ашиглаж болно.

6.1-р хэсэгт текст нь үндсэн замын баталгаажуулалтыг тайлбарласан болно. Хүчин төгөлдөр замууд нь итгэмжлэгдсэн талуудаас олгосон гэрчилгээнээс эхэлдэг. Алгоритм нь ГОБ-ын нийтийн түлхүүр, ГОБ-ын нэр болон энэ түлхүүрийг ашиглан баталгаажуулж болох замуудын багцад тавигдах аливаа хязгаарлалтыг шаарддаг.

Итгэмжлэгдсэн талыг сонгох нь бодлогын асуудал юм: энэ нь шаталсан НТДБ дахь дээд түвшний ГОБ, баталгаажуулагчийн өөрийн гэрчилгээ(үүд)-ийг олгосон ГОБ эсвэл НТДБ сүлжээн дэх бусад ГОБ байж болно. Замын баталгаажуулалтын процедур нь итгэлцлийн талыг сонгохоос үл хамааран ижил байна. Нэмж дурдахад, өөр өөр аппликейшн нь өөр өөр итгэлцлийн талууд дээр тулгуурлаж болно, эсвэл итгэлцлийн талын аль нэгээр эхэлдэг замыг

хүлээн зөвшөөрч болно.

6.2-т тодорхой хэрэгжилтэд замын баталгаажуулалтын алгоритмыг ашиглах аргуудыг тайлбарласан болно.

6.3-т ХГЖ нь гэрчилгээ олгогчийн хүчингүй болгох механизм байх үед гэрчилгээг хүчингүй болгосон эсэхийг тодорхойлоход шаардлагатай алхмуудыг тайлбарласан болно.

6.1. Үндсэн замын баталгаажуулалт

Энэ текст нь X.509 зам боловсруулах алгоритмыг тайлбарлана. Хамаарах хэрэгжүүлэлт нь энэ алгоритмын гадаад үйлдэлтэй функциональ байдлаар дүйцэх X.509 замыг боловсруулах процедурыг ЗААВАЛ оруулах ёстой. Гэсэн хэдий ч, энэ алгоритмд боловсруулсан гэрчилгээний өргөтгөлүүдийн заримыг дэмжих нь нийцтэй хэрэгжүүлэлтийн хувьд ЗАЙЛШГҮЙ БИШ. Эдгээр өргөтгөлүүдийг дэмждэггүй үйлчлүүлэгчид замын баталгаажуулалтын алгоритмын харгалзах алхмуудыг орхиж болно.

Жишээлбэл, үйлчлүүлэгчид бодлогын зураглалын өргөтгөлийг дэмжих шаардлагагүй. Энэ өргөтгөлийг дэмждэггүй үйлчлүүлэгчид бодлогын зураглалыг боловсруулах замын баталгаажуулалтын алхмуудыг орхиж болно. Дэмжих боломжгүй чухал өргөтгөлтэй бол үйлчлүүлэгчид гэрчилгээг татгалзах ёстой.

Энэхүү стандартын баримт бичгийн 4, 5-р хэсэгт заасан гэрчилгээ болон ХГЖ профайлууд нь гэрчилгээ, ХГЖ талбарууд болон интернэт НТДБ-д тохиромжтой гэж үзсэн өргөтгөлүүдийн утгыг зааж өгсөн боловч энэ хэсэгт үзүүлсэн алгоритм нь зөвхөн гэрчилгээ, эдгээр профайлтай нийцэх ХГЖ хүлээн авахаар зөвхөн хязгаарлагдахгүй.. Тиймээс, алгоритм нь зөвхөн X.509-ийн дагуу баталгаажуулалтын зам хүчинтэй эсэхийг баталгаажуулах шалгалтуудыг багтаасан бөгөөд гэрчилгээ болон ХГЖ-ууд энэ профайлтай нийцэж байгаа эсэхийг шалгах шалгалтуудыг оруулдаггүй. Алгоритмыг 4 ба 5-р хэсэг дэх профайлуудтай нийцэж байгаа эсэхийг шалгахын тулд өргөтгөж болох боловч энэ профайл нь ийм шалгалтыг оруулахгүй байхыг ЗӨВЛӨДӨГ.

Энэ хэсэгт үзүүлсэн алгоритм нь гэрчилгээг одоогийн огноо, цаг хугацааны хувьд баталгаажуулдаг. Хамаарах хэрэгжилт нь өнгөрсөн хугацааны зарим нэг баталгаажуулалтыг дэмжиж болно. Гэрчилгээний хүчинтэй хугацаанаас гаднах хугацаанд гэрчилгээг баталгаажуулах механизм байхгүй гэдгийг анхаарна уу.

Итгэмжлэгдсэн тал нь алгоритмын оролт болно. Бүх гэрчилгээжүүлэлтийн замыг баталгаажуулахын тулд ижил итгэмжлэгдсэн талуудыг ашиглах

шаардлагагүй. Хэсэг 6.2-т дэлгэрэнгүй авч үзсэний дагуу өөр өөр замуудыг баталгаажуулахын тулд өөр өөр итгэмжлэгдсэн талуудыг ашиглаж болно.

Замын баталгаажуулалтын үндсэн зорилго нь итгэмжлэгдсэн талын нийтийн түлхүүр дээр тулгуурлан тухайн гэрчилгээнд дүрслэгдсэн субъектийн онцлог нэр эсвэл субъектийг өөр нэр болон субъектийн нийтийн түлхүүрийн хоорондын уялдаа холбоог шалгах явдал юм. Ихэнх тохиолдолд зорилтот гэрчилгээ нь эцсийн байгууллагын гэрчилгээ байх боловч нийтийн түлхүүрийн гэрчилгээний гарын үсгийг баталгаажуулахаас өөр зорилгоор ашиглах тохиолдолд зорилтот гэрчилгээ нь ГОБ-ын гэрчилгээ байж болно. Нэр болон субъектийн нийтийн түлхүүрийн хоорондох холбоосыг шалгахын тулд уг холболтыг дэмжих гэрчилгээний дарааллыг тодорхойлох шаардлагатай. Энэхүү дарааллын гэрчилгээг авахын тулд гүйцэтгэсэн процедур нь энэ тодорхойлолтын хамрах хүрээнээс гадуур байна.

Энэ зорилгод хүрэхийн тулд замын баталгаажуулалтын үйл явц нь бусад зүйлсээс гадна ирээдүйн баталгаажуулалтын зам (n гэрчилгээний дараалал) нь дараах нөхцөлийг хангасан эсэхийг баталгаажуулна.

A) {1, ..., n-1} дэх бүх x-ийн хувьд x гэрчилгээний субъект нь x+1 гэрчилгээ олгогч байна;

B) 1-р гэрчилгээг итгэмжлэгдсэн талаас олгосон;

C) Гэрчилгээ n нь баталгаажуулах гэрчилгээ (өөрөөр хэлбэл зорилтот гэрчилгээ); болон

D) {1, ..., n} дахь бүх x-ийн хувьд гэрчилгээ тухайн үед хүчинтэй байсан.

Гэрчилгээ нь ирээдүйн баталгаажуулалтын замд нэгээс олон удаа гарч ирж болохгүй.

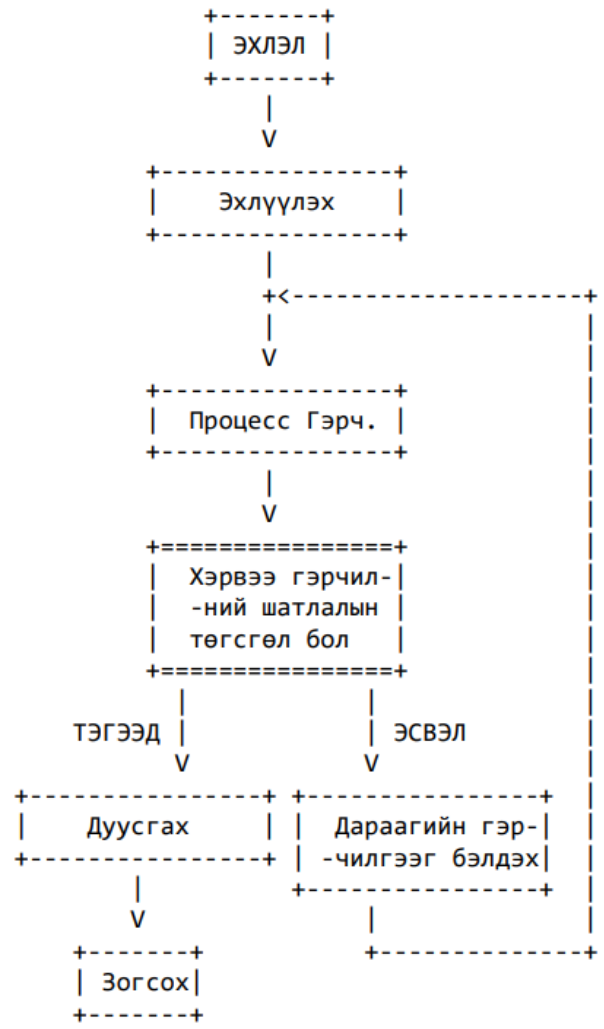
Итгэмжлэгдсэн тал нь өөрөө өөртөө гарын үсэг зурсан гэрчилгээ хэлбэрээр өгөх үед энэхүү өөрөө гарын үсэг зурсан гэрчилгээг ирээдүйн гэрчилгээжүүлэлтийн замын нэг хэсэг болгон оруулахгүй. Итгэмжлэгдсэн талуудын талаарх мэдээллийг гэрчилгээжүүлэлтийн замын баталгаажуулалтын алгоритмын оролт болгон өгнө (Хэсэг 6.1.1).

Гэрчилгээжүүлэх тухайн зам нь бүх аппликейшнд тохирохгүй байж болно. Тиймээс, аппликейшн нь хүчинтэй замуудын багцыг хязгаарлахын тулд энэ алгоритмыг өргөтгөх боломжтой. Замын баталгаажуулалтын процедур нь гэрчилгээний бодлогын өргөтгөл, бодлогын зураглалын өргөтгөл, бодлогын хязгаарлалтын өргөтгөл болон anyPolicy өргөтгөлийг хориглох зэрэгт үндэслэн

энэ замд хүчинтэй гэрчилгээний бодлогыг тодорхойлдог. Үүнд хүрэхийн тулд зам баталгаажуулалтын алгоритм нь хүчинтэй бодлогын модыг бүтээдэг. Хэрэв энэ замын хувьд хүчинтэй гэрчилгээний бодлогын багц хоосон биш бол үр дүн нь n гүнтэй хүчинтэй бодлогын мод байх ба үгүй бол үр дүн нь хоосон хүчинтэй бодлогын мод байх болно.

Хэрэв субъект болон ГО-ийн талбарт ижил ЯН гарч ирвэл гэрчилгээг өөрөө олгоно (хэрэв 7.1-д заасан дүрэмд нийцэж байвал хоёр ЯН нь ижил байна). Ерөнхийдөө зам бүрдүүлж буй гэрчилгээ олгогч болон субъект нь гэрчилгээ бүрийн хувьд өөр өөр байдаг. Гэсэн хэдий ч, ГОБ нь түлхүүр шилжүүлэлт эсвэл гэрчилгээний бодлогын өөрчлөлтийг дэмжих зорилгоор өөртөө гэрчилгээ олгож болно. Замын урт эсвэл нэрийн хязгаарлалтыг үнэлэхэд эдгээр өөрөө олгосон гэрчилгээг тооцохгүй.

Энэ хэсэгт алгоритмыг дөрвөн үндсэн үе шаттайгаар үзүүлэв: (1) эхлүүлэх, (2) гэрчилгээний үндсэн боловсруулалт, (3) дараагийн гэрчилгээнд бэлтгэх, (4) Гэрчилгээжүүлэх. (1) ба (4) алхмуудыг яг нэг удаа гүйцэтгэнэ. Алхам (2) нь тухайн зам дээрх бүх гэрчилгээнд хийгдэнэ. Алхам (3) нь эцсийн гэрчилгээнээс бусад зам дээрх бүх гэрчилгээнд хийгдэнэ. Зураг 2-т энэ алгоритмын өндөр түвшний урсгал диаграммыг үзүүлэв.



Зураг 2. Гэрчилгээжүүлэлтийн зам боловсруулах урсгал диаграмм

6.1.1. Оролтууд

Энэхүү алгоритм нь зам боловсруулах логикт дараах есөн оролтыг авч үздэг.

A) n урттай ирээдүйн гэрчилгээжүүлэлтийн зам.

B) Одоогийн огноо/цаг.

C) Хэрэглэгчийн-эхлэлийн-бодлогын-багц: Хэрэглэгчдэд хүлээн зөвшөөрөгдсөн бодлогыг нэрлэсэн гэрчилгээний бодлого тодорхойлогчдын багц. Хэрэв хэрэглэгч гэрчилгээний бодлогод санаа зовохгүй байвал хэрэглэгчийн-эхлэлийн-бодлогын-багц нь any-policy гэсэн тусгай утгыг агуулна.

D) Гэрчилгээжүүлэлтийн замд итгэмжлэгдсэн тал болж үйлчилгээ үзүүлж буй ГОБ-г тодорхойлсон итгэмжлэгдсэн талын мэдээлэл. Итгэмжлэгдсэн талын мэдээлэлд дараах зүйлс орно.

1) итгэмжлэгдсэн олгогчийн нэр,
2) итгэмжлэгдсэн нийтийн түлхүүрийн алгоритм,
3) итгэмжлэгдсэн нийтийн түлхүүр ба
4) сонголтоор, нийтийн түлхүүртэй холбоотой итгэмжлэгдсэн нийтийн түлхүүрийн параметрүүд.

Итгэмжлэгдсэн талын мэдээллийг зам боловсруулах процедурт өөрөө гарын үсэг зурсан гэрчилгээ хэлбэрээр өгч болно. Итгэмжлэгдсэн талын мэдээллийг гэрчилгээ хэлбэрээр өгөх үед субъект талбар дахь нэрийг итгэмжлэгдсэн олгогчийн нэр болгон, SubjectPublicKeyInfo талбарын агуулгыг итгэмжлэгдсэн нийтийн түлхүүрийн алгоритм болон итгэмжлэгдсэн нийтийн түлхүүрийн эх сурвалж болгон ашигладаг. Итгэмжлэгдсэн талын мэдээлэл нь найдвартай учир нь хоёр хүчин зүйлийн адилтган танилтын процедурын дагуу зам боловсруулах процедурыг хэрэгжүүлнэ. Хэрэв итгэмжлэгдсэн нийтийн түлхүүрийн алгоритм нь параметр шаарддаг бол параметрүүдийг итгэмжлэгдсэн нийтийн түлхүүрийн хамт өгнө.

E) эхлэлийн-бодлогын-зураглалын-хориглох, энэ нь гэрчилгээжүүлэлтийн замд бодлогын зураглалыг зөвшөөрсөн эсэхийг харуулдаг.

F) эхлэлийн-тодорхой-бодлого, энэ нь хэрэглэгчийн-эхлэлийн-бодлогын-багцын гэрчилгээний бодлогын багадаа нэгнийх нь хувьд зам хүчинтэй байх ёстой эсэхийг заадаг.

G) initial-any-policy-inhibit, anyPolicy ОА-г гэрчилгээнд оруулсан бол түүнийг боловсруулах шаардлагатай эсэхийг заадаг.

H) initial-permitted-subtrees (анхны зөвшөөрөгдсөн дэд моднууд) (жишээ нь, X.500 онцолсон нэр, и-мэйл хаяг эсвэл IP хаяг) гэрчилгээжүүлэлтийн зам дахь гэрчилгээ бүрийн бүх субъектийн нэрүүдийг ЗААВАЛ багтаасан дэд модны багцыг заадаг. Анхдагч-зөвшөөрөгдсөн-дэд-модны оролт нь нэр төрөл бүрийн багцыг агуулна. Нэрийн төрөл бүрийн хувьд уг олонлог нь тухайн нэрийн төрлийн бүх нэрийг агуулсан нэг дэд мод, эсвэл тус бүр нь тухайн нэрийн төрлийн нэрсийн дэд олонлогийг зааж өгдөг нэг буюу хэд хэдэн дэд модноос бүрдэх эсвэл олонлог хоосон байж болно. Хэрэв нэрийн төрлийн багц хоосон байвал гэрчилгээжүүлэлтийн зам дахь аливаа гэрчилгээ нь тухайн нэр төрлийн нэрийг агуулсан байвал гэрчилгээжүүлэлтийн замыг хүчингүйд тооцно.

I) initial-excluded-subtrees (анхны-хасагдсан дэд моднууд) (жишээ нь, X.500 онцолсон нэр, и-мэйл хаяг эсвэл IP хаяг) гэрчилгээжүүлэлтийн замд ямар ч

гэрчилгээний субъектийн нэр орохгүй байх дэд модны багцыг заадаг. Анхдагч-хасаагдсан-дэд модны оролт нь нэр төрөл бүрийн багцыг агуулна. Нэрийн төрөл бүрийн хувьд багц нь хоосон байж болно, эсвэл тус бүр нь тухайн нэрийн төрлийн нэрсийн дэд олонлогийг тодорхойлсон нэг буюу хэд хэдэн дэд модноос бүрдэж болно. Хэрэв нэрийн төрлийн багц хоосон байвал тухайн нэр төрлийн нэрсийг оруулахгүй.

Эдгээр бүх оролтын тохиргоог дэмжихийн тулд хамаарах хэрэгжилт шаардлагагүй. Жишээ нь, нийцсэн хэрэгжүүлэлт нь анхдагч-ямар-бодлогыг хориглох-д FALSE-ийн утгыг ашиглан баталгаажуулалтын бүх замыг баталгаажуулах зорилготой байж болно.

6.1.2. Эхлүүлэх

Энэхүү эхлүүлэх үе шат нь есөн оролт дээр үндэслэн арван нэгэн төлөвийн хувьсагчийг үүсгэнэ:

A) valid_policy_tree (хүчинтэй_бодлогын_мод): Шалгуур үзүүлэлт бүхий гэрчилгээний бодлогын мод; модны навч бүр нь гэрчилгээжүүлэлтийн замын баталгаажуулалтын энэ үе шатанд хүчинтэй бодлогыг илэрхийлдэг. Хэрэв гэрчилгээжүүлэлтийн замын баталгаажуулалтын тухайн үе шатанд хүчинтэй бодлого байгаа бол модны гүн нь боловсруулсан гинжин хэлхээний гэрчилгээний тоотой тэнцүү байна. Хэрэв гэрчилгээжүүлэлтийн замын баталгаажуулалтын тухайн үе шатанд хүчинтэй бодлого байхгүй бол модыг NULL болгож тохируулна. Модыг NULL болгож тохируулсны дараа бодлогын боловсруулалтыг зогсооно.

Хүчинтэй_бодлогын_модны зангилаа бүр нь хүчинтэй бодлого, холбогдох бодлогын шалгуур үзүүлэлт, нэг буюу хэд хэдэн the expected_policy_set (хүлээгдэж буй бодлогын багц) гэсэн гурван өгөгдлийн объектыг агуулна. Хэрэв зангилаа х гүнд байвал зангилааны бүрэлдэхүүн хэсгүүд нь дараах семантиктай байна.

1) Хүчинтэй_бодлого нь х урттай замын хүчинтэй бодлогыг илэрхийлдэг ганц бодлогын ОА юм.

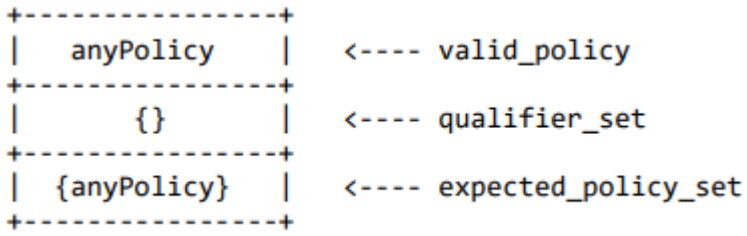
2) Qualifier_set (шалгуур үзүүлэлтийн багц) нь х гэрчилгээ дэх хүчинтэй бодлоготой холбоотой бодлогын шалгуур үзүүлэлтүүдийн багц юм.

3) expected_policy_set (Хүлээгдэж буй_бодлогын багц) нь х+1 гэрчилгээнд энэ бодлогыг хангах нэг буюу хэд хэдэн бодлогын ОА-г агуулна.

Хүчинтэй_бодлогын_модны анхны утга нь valid_policy anyPolicy-тай нэг

зангилаа, хоосон шалгуурын_иж бүрдэл, anyPolicy ганц утгатай хүлээгдэж буй_бодлогын_багц юм. Энэ зангилааг тэг гүнд гэж үзнэ.

Зураг 3 нь хүчинтэй_бодлогын_модны анхны төлөвийн график дүрслэл юм. Зам боловсруулах явцад хүчинтэй_бодлогын_модны өөрчлөлтийг тайлбарлахын тулд нэмэлт тоо баримтууд энэ форматыг ашиглана.



Зураг 3. Хүчинтэй_бодлогын_модны төлөвийн хувьсагчийн анхны утга

B) permitted_subtrees (зөвшөөрөгдсөн_дэд мод): Нэрийн төрөл тус бүрийн эх үүсвэрийн нэрсийн багц (жишээ нь, X.500 ялгагдах нэр, и-мэйл хаяг эсвэл IP хаяг) нь гэрчилгээжүүлэлтийн зам дахь дараагийн гэрчилгээ дэх бүх субъектийн нэр ЗААВАЛ багтах дэд модны багцыг тодорхойлдог. Энэ хувьсагч нь нэр төрөл бүрийн олонлогийг агуулдаг бөгөөд анхны утга нь анхны зөвшөөрөгдсөн дэд мод байна.

C) Excluded_subtrees (хасагдсан_дэд мод): нэрийн төрөл тус бүрийн язгуур нэрсийн багц (жишээ нь, X.500 онцолсон нэр, и-мэйл хаяг эсвэл IP хаяг) нь гэрчилгээжүүлэлтийн зам дахь дараагийн гэрчилгээнүүдийн субъектийн нэргүй дэд модны багцыг тодорхойлдог. Энэ хувьсагч нь нэр төрөл бүрийн олонлогийг агуулдаг бөгөөд анхны утга нь эхний-хасагдсан-дэд мод байна.

D) Explicit_policy (тодорхой_бодлого): NULL биш valid_policy_tree (хүчинтэй_бодлогын-мод) шаардлагатай эсэхийг харуулдаг бүхэл тоо. Бүхэл тоо нь энэ шаардлагыг тавихаас өмнө өөрөө өөртөө олгогдоогүй гэрчилгээний тоог заана. Нэгэнт тохируулсны дараа энэ хувьсагчийг бууруулж болох ч нэмэгдүүлэх боломжгүй. Өөрөөр хэлбэл, хэрэв зам дээрх гэрчилгээ нь NULL биш хүчинтэй_бодлогын модыг шаарддаг байвал дараагийн гэрчилгээ нь энэ шаардлагыг үгүйсгэх боломжгүй. Хэрэв анхдагч-тодорхой-бодлогыг тохируулсан бол анхны утга нь 0, үгүй бол анхны утга нь n+1 байна.

E) inhibit_anyPolicy: anyPolicy бодлогын адилтгагч нь таарч байгаа эсэхийг харуулах бүхэл тоо. Хэрэв дундын өөрөө олгосон гэрчилгээнээс өөр гэрчилгээнд нотлогдсон бол anyPolicy ОА-г өмнө боловсруулах өөрөө өөртөө олгоогүй гэрчилгээний тоог заах бүхэл тоог орхино. Нэгэнт

тохируулсны дараа энэ хувьсагчийг бууруулж болох ч нэмэгдүүлэхгүй байж болно. Өөрөөр хэлбэл, зам дээрх гэрчилгээ нь аливаа бодлогыг боловсруулахад саад учруулж байвал дараагийн гэрчилгээ нь үүнийг зөвшөөрөхгүй. Хэрэв initial-any-policy-inhibit тохируулагдсан бол анхны утга нь 0, үгүй бол анхны утга нь n+1 байна.

F) Policy_mapping (бодлогын_зураглал): бодлогын зураглалыг зөвшөөрөгдсөн эсэхийг тодорхойлдог бүхэл тоо. Бүхэл тоо нь бодлогын зураглалыг хориглохоос өмнө боловсруулах ёстой өөрөө өөртөө олгоогүй гэрчилгээний тоог заана. Нэгэнт тохируулсны дараа энэ хувьсагчийг бууруулж болох ч нэмэгдүүлэхгүй байж болно. Өөрөөр хэлбэл, зам дээрх гэрчилгээ нь бодлогын зураглалыг зөвшөөрөхгүй гэж заасан бол дараачийн гэрчилгээгээр үүнийг хүчингүй болгох боломжгүй. Хэрэв initial-policy-mapping-inhibit тохируулагдсан бол анхны утга нь 0, үгүй бол анхны утга нь n+1 байна.

G) Working_public_key_algorithm (ажиллаж_буй_нийтийн_түлхүүр_алгоритм): гэрчилгээний гарын үсгийг баталгаажуулахад ашигладаг тоон гарын үсгийн алгоритм. Ажиллаж_буй_нийтийн_түлхүүр_алгоритм нь итгэмжлэгдсэн талын мэдээллээр тодорхойлогдсон итгэмжлэгдсэн нийтийн түлхүүрийн алгоритмаас эхэлнэ.

H) Working_public_key (Ажиллаж_буй_нийтийн_түлхүүр): гэрчилгээний гарын үсгийг баталгаажуулахад ашигладаг нийтийн түлхүүр. Ажиллаж_буй_нийтийн_түлхүүрийг итгэмжлэгдсэн талын мэдээллээр тодорхойлогдсон итгэмжлэгдсэн нийтийн түлхүүрээс эхлүүлнэ.

I) Working_public_key_parameters (ажлын_нийтийн_түлхүүр_параметрүүд): гарын үсгийг баталгаажуулахад шаардлагатай байж болох одоогийн нийтийн түлхүүртэй холбоотой параметрүүд (алгоритмаас хамаарч). Ажиллах_нийтийн_түлхүүр_параметрийн хувьсагчийг итгэмжлэгдсэн талын мэдээллээр тодорхойлогдсон итгэмжлэгдсэн нийтийн түлхүүрийн параметрүүдээс эхлүүлнэ.

J) Working_issuer_name (Ажиллаж_буй_олгогчийн_нэр): гинжин хэлхээний дараагийн гэрчилгээнд хүлээгдэж буй ГО-ийн нэр. Ажиллаж_буй_олгогчийн_нэр нь итгэмжлэгдсэн талын мэдээллээр тодорхойлогдсон итгэмжлэгдсэн олгогчийн нэр байна.

K) Max_path_length (хамгийн их_замын_урт): энэ бүхэл тоо нь n-ээр эхэлж, зам дахь өөрөө өөртөө олгоогүй гэрчилгээ бүрийн хувьд буурч, ГОБ-ын үндсэн хязгаарлалтын өргөтгөлийн хүрээн дэх замын уртын хязгаарлалтын талбар

дахь утга хүртэл буурч болно.

Эхлэх алхмууд дууссаны дараа 6.1.3-т заасан гэрчилгээ боловсруулах үе шатуудын дараагийн алхам болох үндсэн гэрчилгээ боловсруулах үйлдлийг гүйцэтгэнэ.

6.1.3. Үндсэн гэрчилгээ боловсруулах

Гэрчилгээ i (i нь [1..n] утгатай)-ын хувьд үндсэн зам боловсруулах үйлдлүүдийг доор жагсааж үзүүлэв.

A) Үндсэн гэрчилгээний мэдээллийг баталгаажуулах. Гэрчилгээ нь дараах зүйлсийг хангасан байх ёстой. Үүнд:

1) Ажиллаж_буй_нийтийн_түлхүүр_алгоритм, Ажиллаж_буй_нийтийн_түлхүүр болон ажиллаж буй_нийтийн_түлхүүр_параметрүүдийг ашиглан гэрчилгээ дээрх гарын үсгийг шалгах боломжтой.

2) Гэрчилгээ хүчинтэй байх хугацаа нь одоогийн цагийг агуулна.

3) Одоогийн байдлаар гэрчилгээг хүчингүй болгоогүй байна. Үүнийг тохирох ХГЖ (6.3-р хэсэг), статусын мэдээллээр эсвэл хоёр хүчин зүйлийн адилтган танилтын механизмаар тодорхойлж болно.

4) Гэрчилгээ олгогчийн нэр нь ажиллаж_буй_олгогчийн_нэр юм.

B) Хэрэв i гэрчилгээ өөрөө өөртөө олгогдсон бөгөөд энэ нь зам дээрх эцсийн гэрчилгээ биш бол i гэрчилгээ авахын тулд энэ алхмыг алгасах. Үүгүй бол субъектийн нэр X.500 нэрний зөвшөөрөгдсөн дэд модны аль нэгэнд байгаа эсэхийг шалгах ба subjectAltName өргөтгөлийн (чухал эсвэл чухал биш) өөр нэр тус бүр нь тухайн нэрийн төрлийн зөвшөөрөгдсөн_дэд модны аль нэгэнд байгаа эсэхийг шалгах.

C) Хэрэв i гэрчилгээ өөрөө өөртөө олгогдсон бөгөөд энэ нь зам дээрх эцсийн гэрчилгээ биш бол i гэрчилгээ авахын тулд энэ алхмыг алгасах. Үүгүй бол, субъектийн нэр X.500 нэрийн хасагдсан_дэд модны аль нэгэнд байхгүй байгаа эсэхийг шалгах ба subjectAltName өргөтгөлийн (чухал эсвэл чухал биш) өөр нэр тус бүр нь тухайн нэрийн төрлийн хасагдсан_дэд модны аль нэгэнд байхгүй байгаа эсэхийг шалгах.

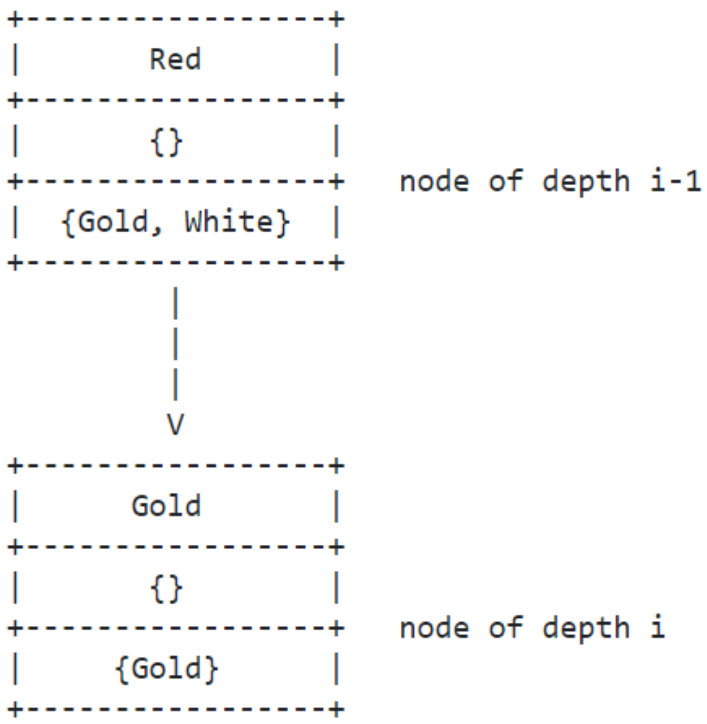
D) Гэрчилгээнд гэрчилгээний бодлогын өргөтгөл дүрслэгдсэн бөгөөд valid_policy_tree нь NULL биш бол дараах алхмуудын дагуу бодлогын мэдээллүүдийг боловсруулна. Үүнд:

1) Гэрчилгээний бодлогын өргөтгөлийн anyPolicy-тай тэнцүү биш P

бодлого бүрийн хувьд P-OID нь P бодлогын OID, P-Q нь P бодлогын шалгах үзүүлэлтийн багц гэж тэмдэглэе.

- P-OID хүлээгдэж буй_бодлогын багцад байгаа хүчинтэй_бодлогын_модны i-1 гүнтэй зангилаа бүрийн хувьд дараах хэлбэрээр хүүхэд зангилаа үүсгэнэ: хүчинтэй_бодлогыг P-OID, шалгуур үзүүлэлтийг P-Q болгож, хүлээгдэж буй_бодлогын багцыг { P-OID} гэж тохируулна.

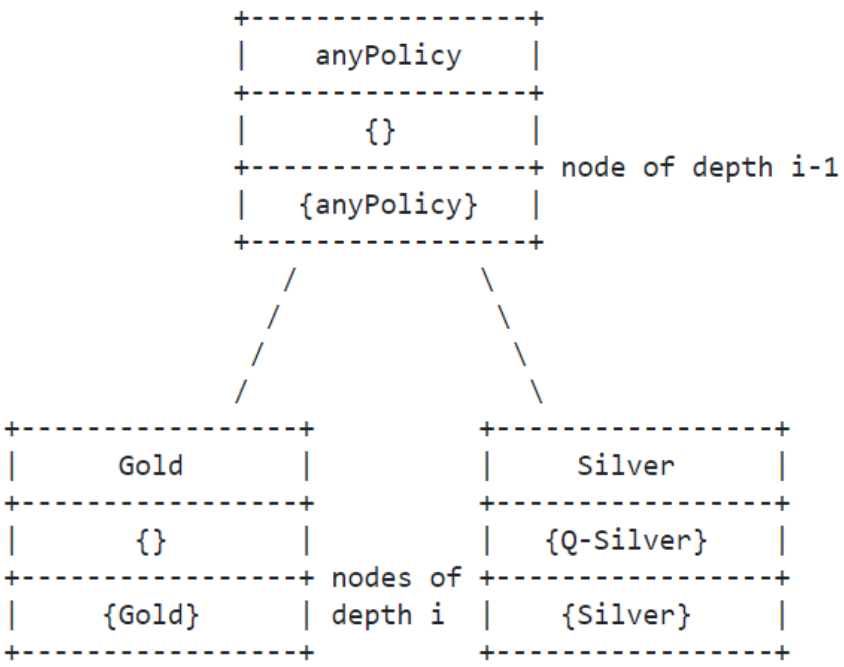
  Жишээ нь, хүлээгдэж буй_бодлогын багц нь {Алт, Цагаан} i-1 гүнийн зангилаатай хүчинтэй_бодлогын_модыг авч үзье. Гэрчилгээ i-нь гэрчилгээний бодлогын өргөтгөлд Алт, Мөнгө гэсэн гэрчилгээний бодлого гарч ирнэ гэж бодъё. Алтны бодлого таарч байгаа ч Мөнгөний бодлого таарахгүй. Энэ дүрэм нь алтны бодлогод i гүний хүүхэд зангилааг үүсгэнэ. Үр дүнг Зураг 4-т үзүүлэв.



Зураг 4. Яг тохирохыг боловсруулж байна

- Хэрэв (i) алхамд тохирох зүйл байхгүй бөгөөд valid_policy_tree (хүчинтэй_бодлогын_мод) нь valid_policy anyPolicy-тай i-1 гүнтэй зангилаа агуулж байвал дараах утгуудтай хүүхэд зангилаа үүсгэнэ: valid_policy-г P-OID болгож, qualifier_set-г тохируулна. P-Q ба хүлээгдэж буй_бодлогын багцыг {P-OID} болгож тохируулна.

Жишээ нь, valid_policy хүчинтэй_бодлого нь anyPolicy байх i-1 гүнийн зангилаатай valid_policy_tree хүчинтэй_бодлогын модыг авч үзье. Гэрчилгээ i-ын гэрчилгээний бодлогын өргөтгөлд Алт, Мөнгө гэсэн гэрчилгээний бодлого гарч ирнэ гэж бодъё. Алт бодлогод шалгуур үзүүлэлт байхгүй, харин Мөнгөн бодлогод Q-Silver шалгуур үзүүлэлт байдаг. Дээрх (i)-д алт, мөнгө тараагүй бол энэ процедур нь бодлого тус бүрд нэг i гүнтэй хоёр хүүхэд зангилааг үүсгэнэ. Үр дүнг 5-р зурагт үзүүлэв.



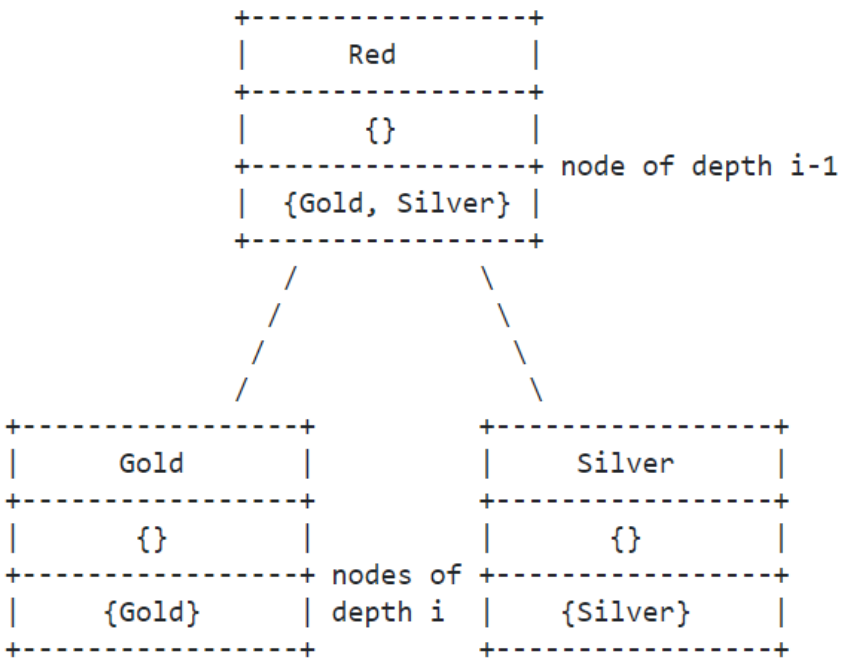
Зураг 5. Leaf Node нь anyPolicy-ыг тодорхойлж байхад Үл тохирох бодлогуудыг боловсруулж байна

2) Хэрэв гэрчилгээний бодлогын өргөтгөл нь AP-Q шалгуур үзүүлэлт бүхий anyPolicy бодлогыг агуулж байгаа бөгөөд (a) inhibit_anyPolicy нь 0-ээс их эсвэл (b) i<n бөгөөд гэрчилгээ өөрөө олгосон бол:

i-1 гүнтэй хүчинтэй_бодлогын_модны зангилаа тус бүрийн хувьд хүлээгдэж буй_бодлогын багц дахь (ямар ч бодлогыг оруулаад) хүүхэд зангилаанд харагдахгүй байгаа утга бүрийн хувьд дараах утгуудтай хүүхэд зангилаа үүсгэнэ үү: хүчинтэй_бодлогыг хүлээгдэж буй_бодлогын багцын утгад тохируулна уу. эх зангилаа, qualifier_set-ийг AP-Q болгож тохируулж, хүлээгдэж буй_бодлогын багцыг энэ зангилаанаас хүчинтэй_бодлогын утгад тохируулна уу.

Жишээ нь, хүлээгдэж буй_бодлогын багц нь {Алт, Мөнгө} байх i-1

гүнийн зангилаатай хүчинтэй_бодлогын модыг авч үзье. Гэрчилгээ i-н гэрчилгээний өргөтгөлд ямар ч бодлого шалгуур үзүүлэлтгүйгээр anyPolicy гарч ирсэн ч алт, мөнгө харагдахгүй байна гэж бодъё. Энэ дүрэм нь бодлого тус бүрд нэг i гүнтэй хоёр хүүхэд зангилааг үүсгэнэ. Үр дүнг 6-р зурагт үзүүлэв.



Зураг 6. Гэрчилгээний бодлогын өргөтгөл anyPolicy-ыг тодорхойлж байхад Үл тохирох бодлогуудыг боловсруулж байна

3) Хэрэв i-1 эсвэл түүнээс бага гүнд valid_policy_tree (хүчинтэй_бодлогын_мод)-д ямар ч хүүхэд зангилаагүй зангилаа байгаа бол бол уг зангилааг устгана. Хүүхэдгүйгээр i-1 ба түүнээс бага гүнтэй зангилаа байхгүй болтол энэ алхмыг давтана.

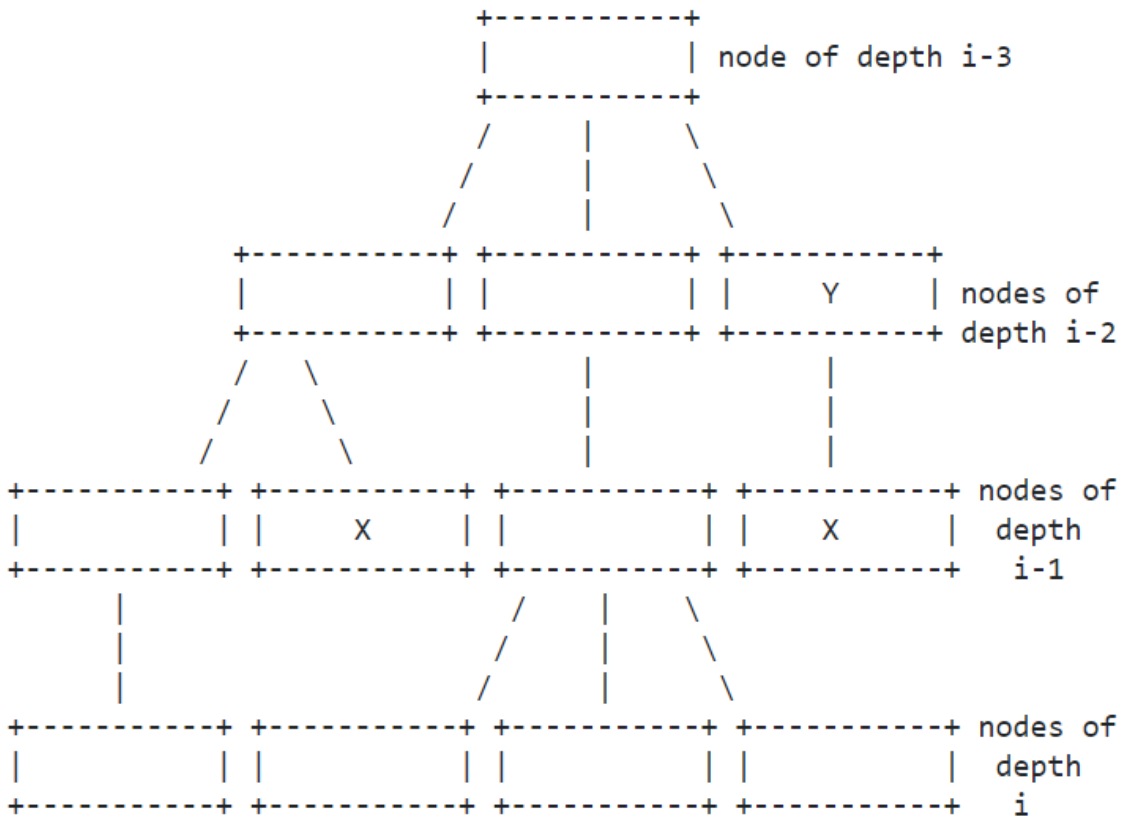
   Жишээлбэл, доорх Зураг 7-д үзүүлсэн valid_policy_tree (хүчинтэй_бодлогын_мод)-ыг авч үзье. 'X' гэж тэмдэглэгдсэн i-1 гүн дэх хоёр зангилаа нь хүүхэдгүй бөгөөд тэдгээрийг устгасан. Үүссэн модонд энэ дүрмийг хэрэглэснээр 'Y' тэмдэглэгдсэн i-2 гүн дэх зангилаа устах болно. Үүссэн модонд хүүхэдгүй i-1 ба түүнээс бага гүнтэй зангилаа байхгүй бөгөөд энэ алхмыг дуусгана.

E) Хэрэв гэрчилгээний бодлогын өргөтгөл байхгүй бол valid_policy_tree (хүчинтэй_бодлогын_мод)-ыг NULL болгож тохируулна.

F) Explicit_policy (Тодорхой_бодлого)-ын аль нэг нь 0-ээс их эсвэл valid_policy_tree (хүчинтэй_бодлогын_мод) нь NULL-тэй тэнцүү биш эсэхийг шалгах;

Хэрэв (a), (b), (c), (f) алхмуудын аль нэг нь амжилтгүй болбол процедур дуусгавар болж, алдааны шинж тэмдэг болон зохих шалтгааныг буцаана.

Хэрэв i нь n-тэй тэнцүү биш бол 6.1.4-т жагсаасан бэлтгэл алхмуудыг хийж үргэлжлүүлнэ. Хэрэв i нь n-тэй тэнцүү бол 6.1.5-р хэсэгт жагсаасан дуусгах алхмуудыг гүйцэтгэнэ.



Зураг 7. хүчинтэй_бодлогын_модыг тайрах

6.1.4. Гэрчилгээ i+1-ыг боловсруулахад бэлтгэх

i+1 гэрчилгээг боловсруулахад бэлтгэхийн тулд i гэрчилгээний хувьд дараах алхмуудыг гүйцэтгэнэ.

A) Хэрэв бодлогын зураглалын өргөтгөл байгаа бол anyPolicy тусгай утга нь issuerDomainPolicy эсвэл SubjectDomainPolicy шиг харагдахгүй байгаа эсэхийг шалгах.

B) Хэрэв бодлогын зураглалын өргөтгөл байгаа бол бодлогын зураглалын өргөтгөл доторх issuerDomainPolicy ID-P тус бүрийн хувьд:

1) Policy_mapping хувьсагч 0-ээс их байвал ID-P нь valid_policy (хүчинтэй_бодлого) байх i гүнийн valid_policy_tree

(хүчинтэй_бодлогын_мод)-ны зангилаа бүрийн хувьд expected_policy_set (хүлээгдэж буй_бодлогын багц)-ыг бодлогын зураглалын өргөтгөлөөр ID-P-тэй дүйцэхүйц гэж заасан subjectDomainPolicy утгуудад тохируулна.

Хэрэв valid_policy_tree (хүчинтэй_бодлогын_мод)-ны I гүний зангилаа нь ID-P-ийн valid_policy (хүчинтэй_бодлого)-гүй боловч anyPolicy-ийн valid_policy (хүчинтэй_бодлого)-той i гүнийн зангилаа байгаа бол i-1 гүнийн зангилааны хүүхэд зангилааг дараах байдлаар үүсгэнэ. Үүнд:

- valid_policy (хүчинтэй_бодлого)-ыг ID-P болгож тохируулах;
- i гэрчилгээний гэрчилгээний бодлогын өргөтгөл дэх anyPolicy бодлогын шалгуурын багцад qualifier_set-ийг тохируулах; болон
- бодлогын зураглалын өргөтгөлөөр ID-P-тэй дүйцэхүйц гэж заасан subjectDomainPolicy утгуудын багцад хүлээгдэж буй_бодлогын багцыг тохируулна.

2) Хэрэв policy_mapping хувьсагч 0-тэй тэнцүү бол:

- ID-P нь valid_policy (хүчинтэй_бодлого) байх valid_policy_tree (хүчинтэй_бодлогын_мод)-дахь i гүний зангилаа бүрийг устгана.
- Хэрэв valid_policy_tree (хүчинтэй_бодлогын_мод)-ны гүнд i-1 ба түүнээс бага хэмжээтэй зангилаа байгаа бол ямар ч хүүхэд зангилаагүй бол уг зангилааг устгана. Хүүхэд заншилаагүй i-1 ба түүнээс бага гүнтэй зангилаа байхгүй болтол энэ алхамыг давтана.

C) Гэрчилгээ олгогчийн нэрийг ажиллаж_буй_олгогчийн_нэр болгож олгоно.

D) Гэрчилгээний subjectPublicKey-г ажиллаж_буй_нийтийн_түлхүүрт олгоно.

E) Хэрэв гэрчилгээний subjectPublicKeyInfo талбар нь хоосон бус параметр бүхий алгоритмын талбарыг агуулж байгаа бол параметрүүдийг work_public_key_parameters хувьсагчдад олгоно.

Хэрэв гэрчилгээний subjectPublicKeyInfo талбарт non-null параметрууд бүхий алгоритмын талбар байгаа эсвэл параметрүүдийг орхигдуулсан бол гэрчилгээний subjectPublicKey алгоритмыг working_public_key_algorithm-тай харьцуулна. Хэрэв гэрчилгээний subjectPublicKey алгоритм болон working_public_key_algorithm (ажиллаж_буй_нийтийн_түлхүүр_алгоритм) нь

ялгаатай бол working_public_key_parameters (ажлын_нийтийн_түлхүүр_параметр)-үүдийг null болгож тохируулна.

F) Гэрчилгээний subjectpublickey алгоритмыг Working_public_key-algorithm (Ажиллаж_буй_нийтийн_түлхүүр_алгоритм)-ын хувьсагчид олгоно.

G) Хэрэв нэрийн хязгаарлалтын өргөтгөлийг гэрчилгээнд оруулсан бол permitted_subtrees (зөвшөөрөгдсөн_дэд_мод) ба excluded_subtrees (хасагдсан_ дэд_мод) төлөвийн хувьсагчдыг дараах байдлаар өөрчилнө. Үүнд:

   1) Хэрэв гэрчилгээнд permittedSubtrees байгаа бол permitted_subtrees төлөвийн хувьсагчийг өмнөх утга болон өргөтгөлийн талбарт заасан утгын огтлолцолд тохируулна. Хэрэв permittedSubtrees нь тодорхой нэрийн төрлийг агуулаагүй бол permitted_subtrees төлөвийн хувьсагч тухайн нэрийн төрлийг өөрчлөхгүй. Жишээлбэл, example.com болон foo.example.com-ын огтлолцол нь foo.example.com юм. example.com болон example.net хоёрын огтлолцол нь хоосон багц юм.

   2) Хэрэв excludedSubtrees гэрчилгээнд байгаа бол excluded_subtrees төлөвийн хувьсагчийг өмнөх утга болон өргөтгөлийн талбарт заасан утгын нэгдэлд тохируулна. Хэрэв excludedSubtrees нь тодорхой нэрийн төрлийг агуулаагүй бол excluded_subtrees төлөвийн хувьсагч тухайн нэрийн төрлийг өөрчлөхгүй. Тухайлбал, нэгдэл example.com болон foo.example.com зайн нэр нь example.com юм. example.com болон example.net хоёрын нэгдэл нь хоёулаа нэрийн орон зай юм.

H) Хэрэв i гэрчилгээг өөрөө өөртөө олгоогүй бол:

   1) Хэрэв explicit_policy (тодорхой_бодлого) 0 биш бол explicit_policy (тодорхой_бодлого)-ыг 1-ээр бууруулна.

   2) Policy_mapping (Бодлогын_зураглал) 0 биш бол Policy_mapping (бодлогын_зураглал)-ыг 1-ээр бууруулна.

   3) Хэрэв inhibit_anyPolicy (хориглосон_дурын_бодлого) 0 биш бол inhibit_anyPolicy-г 1-ээр бууруулна.

I) Хэрэв гэрчилгээнд бодлогын хязгаарлалтын өргөтгөл орсон бол explicit_policy (тодорхой_бодлого)-ын болон Policy_mapping (Бодлогын_зураглал)-ын төлөвийн хувьсагчдыг дараах байдлаар өөрчилнө:

   1) Хэрэв requireExplicitPolicy байгаа бөгөөд explicit_policy (тодорхой_бодлого)-оос бага бол explicit_policy (тодорхой_бодлого)-ыг requireExplicitPolicy-ийн утгад тохируулна.

2) Хэрэв inhibitPolicyMapping байгаа бөгөөд Policy_mapping (Бодлогын_зураглал)-аас бага бол Policy_mapping (Бодлогын_зураглал)-г inhibitPolicyMapping-д тохируулна.

J) Хэрэв inhibitAnyPolicy өргөтгөл нь гэрчилгээнд орсон бөгөөд inhibit_anyPolicy-ээс бага байвал inhibit_anyPolicy-г inhibitAnyPolicy-ийн утгад тохируулна.

K) Хэрэв i гэрчилгээ нь 3-р хувилбарын гэрчилгээ бол basicConstraints өргөтгөл байгаа эсэхийг шалгана, cA-г YHЭH гэж тохируулна. (Хэрэв i гэрчилгээ нь 1-р хувилбар эсвэл 2-р хувилбарын гэрчилгээ бол аппликейшн нь i-р гэрчилгээг ГОБ-ын гэрчилгээ мөн гэдгийг хоёр хүчин зүйлийн адилтган танилтын хэрэгслээр баталгаажуулах эсвэл гэрчилгээнээс татгалзах ёстой. Хамаарах хэрэгжүүлэлт нь бүх хувилбар 1 болон 2-р хувилбарын дунд шатны гэрчилгээнээс татгалзаж болно.)

L) Хэрэв гэрчилгээг өөрөө өөртөө олгоогүй бол max_path_leghth (хамгийн их_замын_урт) тэгээс их байгаа эсэхийг шалгаж, max_path_leghth (хамгийн их_замын_урт)-ыг 1-ээр бууруулна.

M) Хэрэв гэрчилгээнд pathLenConstraint байгаа бөгөөд max_path_length-ээс бага бол max_path_length-г pathLenConstraint-ийн утгад тохируулна.

N) Хэрэв түлхүүрийн хэрэглээний өргөтгөл байгаа бол keyCertSign бит тохируулагдсан эсэхийг шалгана.

O) Гэрчилгээнд байгаа бусад чухал өргөтгөлүүдийг таньж, боловсруулах. Замын боловсруулалттай холбоотой гэрчилгээнд байгаа бусад танигдсан чухал бус өргөтгөлүүдийг боловсруулна.

Хэрэв (a), (k), (l), (n) эсвэл (o) шалгагдаагүй бол процедурыг дуусгаж, алдааны шинж тэмдэг болон зохих шалтгааныг буцаана.

Хэрэв (a), (k), (l), (n), (o) амжилттай дууссан бол i-г нэмэгдүүлж, 6.1.3-т заасан үндсэн гэрчилгээний боловсруулалтыг хийнэ.

6.1.5. Гэрчилгээжүүлэх процедур

Зорилтот гэрчилгээний боловсруулалтыг дуусгахын тулд гэрчилгээ n-ийн хувьд дараах алхмуудыг гүйцэтгэнэ. Үүнд:

A) Хэрэв explicit_policy (тодорхой_бодлого) 0 биш бол explicit_policy (тодорхой_бодлого)-ыг 1-ээр бууруулна.

B) Бодлогын хязгаарлалтын өргөтгөл нь гэрчилгээнд орсон бөгөөд requireExplicitPolicy нь байгаа бөгөөд 0 утгатай бол explicit_policy

(тодорхой_бодлого)-ын төлөвийн хувьсагчийг 0 болгож тохируулна.

C) Гэрчилгээний subjectPublicKey- г ажиллаж_буй_нийтийн_түлхүүрт олгоно.

D) Хэрэв гэрчилгээний subjectPublicKeyInfo талбар нь хоосон бус параметр бүхий алгоритмын талбарыг агуулж байгаа бол параметрүүдийг work_public_key_parameters хувьсагчдад олгоно.

   Хэрэв гэрчилгээний subjectPublicKeyInfo талбарт non-null параметрууд бүхий алгоритмын талбар байгаа эсвэл параметрүүдийг орхигдуулсан бол гэрчилгээний subjectPublicKey алгоритмыг working_public_key_algorithm-тай харьцуулна. Хэрэв гэрчилгээний subjectPublicKey алгоритм болон working_public_key_algorithm (ажиллаж_буй_нийтийн_түлхүүр_алгоритм) нь ялгаатай бол working_public_key_parameters (ажлын_нийтийн_түлхүүр_параметр)-үүдийг null болгож тохируулна.

E) Гэрчилгээний subjectpublickey алгоритмыг Working_public_key-algorithm (Ажиллаж_буй_нийтийн_түлхүүр_алгоритм)-ын хувьсагчид олгоно.

F) Гэрчилгээ n-д байгаа бусад чухал өргөтгөлүүдийг таньж, боловсруулна. Гэрчилгээ n-д байгаа замын боловсруулалттай холбоотой бусад танигдсан чухал бус өргөтгөлүүдийг боловсруулна.

G) Valid_policy_tree (Хүчинтэй_бодлогын_мод) болон user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц)-ын огтлолцлыг дараах байдлаар тооцоолно. Үүнд:

   1) Хэрэв Valid_policy_tree (Хүчинтэй_бодлогын_мод) нь NULL бол огтлолцол нь NULL байна.

   2) Хэрэв Valid_policy_tree (Хүчинтэй_бодлогын_мод) нь NULL биш бөгөөд user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц) нь any_policy (дурын бодлого) бол огтлолцол нь бүхэл Valid_policy_tree (Хүчинтэй_бодлогын_мод) байна.

   3) Хэрэв Valid_policy_tree (Хүчинтэй_бодлогын_мод) нь NULL биш бөгөөд user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц) нь any_policy (дурын бодлого) биш бол Valid_policy_tree (Хүчинтэй_бодлогын_мод) болон user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц)-ын огтлолцлыг дараах байдлаар тооцоолно.

      • Эцэг зангилаа нь anyPolicy-ийн хүчинтэй_бодлоготой бодлогын зангилааны багцыг тодорхойлно. Энэ бол valid_policy_node_set (хүчинтэй_бодлогын_зангилааны багц) юм.

- Хэрэв valid_policy_node_set (хүчинтэй_бодлогын_зангилааны багц)-ын аливаа зангилааны valid_policy (хүчинтэй_бодлого) нь user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц)-д байхгүй бөгөөд anypolicy биш бол энэ зангилаа болон түүний бүх хүүхэд зангилааг устгана.
- Хэрэв Valid_policy_tree (Хүчинтэй_бодлогын_мод)-нд valid_policy anyPolicy-тай n-н гүнтэй зангилаа агуулж байгаа бөгөөд user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц) нь any_policy (дурын бодлого) биш бол дараах алхмуудыг гүйцэтгэнэ:
  - valid_policy anyPolicy-ийн тусламжтайгаар n-н гүнийн зангилааны шалгуурын багц рүү P-Q-г тохируулна.
  - valid_policy_node_set (хүчинтэй_бодлогын_зангилааны багц) дах зангилааны valid_policy (хүчинтэй_бодлого) биш user-initial-policy-set (хэрэглэгчийн анхны бодлогын багц)-ын P-OID бүрийн хувьд valid_policy anyPolicy-тай эцэг нь n-1 гүнийн зангилаа болох хүүхэд зангилааг үүсгэнэ. Хүүхдийн зангилааны утгуудыг дараах байдлаар тохируулна уу: valid_policy (хүчинтэй_бодлого)-ыг P-OID болгож, шалгуур үзүүлэлтийг P-Q болгож, expected_policy (хүлээгдэж буй_бодлого)-ыг {P-OID} болгож тохируулна.
- valid_policy anyPolicy-той n гүнийн зангилааг устгана.

Хэрэв valid_policy_tree (хүчинтэй_бодлогын_мод)-ны n-1 ба түүнээс бага хэмжээтэй гүний хүүхэд зангилаагүй зангилаа байгаа бол уг зангилааг устгана. Хүүхэдгүйгээр n-1 ба түүнээс бага гүнтэй зангилаа байхгүй болтол энэ алхмыг давтана.

Хэрэв (1) explicit_policy (тодорхой_бодлого)-ын хувьсагчийн утга тэгээс их эсвэл (2) valid_policy_tree (хүчинтэй_бодлогын_мод) нь NULL биш байвал замын боловсруулалт амжилттай болно.

6.1.6. Гаралт

Хэрэв замын боловсруулалт амжилттай болбол процедур дуусгавар болж, valid_policy_tree (хүчинтэй_бодлогын_мод), working_public_key (ажиллаж буй_нийтийн_түлхүүр), working_public_key_algorithm

(ажиллаж_буй_нийтийн_түлхүүр_алгоритм) болон working_public_key_parameters (ажиллаж_буй_нийтийн_түлхүүр_параметр)-үүдийн эцсийн утгын хамт амжилттай гэсэн үзүүлэлтийг буцаана.

6.2. Замын баталгаажуулалтын алгоритмын хэрэглээ

Замын баталгаажуулалтын алгоритм нь цор ганц гэрчилгээжүүлэлтийн замыг баталгаажуулах үйл явцыг тодорхойлдог. Гэрчилгээжүүлэлтийн зам бүр нь тодорхой итгэмжлэгдсэн талаас эхэлдэг ч тодорхой системээр баталгаажуулсан бүх гэрчилгээжүүлэлтийн замууд нь нэг итгэмжлэгдсэн талтай байх шаардлагагүй. Нэг буюу хэд хэдэн итгэмжлэгдсэн ГОБ-г сонгох нь дотоод шийдвэр юм. Систем нь өөрийн итгэмжлэгдсэн ГОБ-уудын аль нэгийг нь тодорхой замд найдвартай тал болгон өгч болно. Замын баталгаажуулалтын алгоритмын оролт нь зам бүрийн хувьд ялгаатай байж болно. Замыг боловсруулахад ашигласан оролтууд нь тодорхой итгэмжлэгдсэн талд олгосон итгэлцэл дэх аппликейшны тусгай шаардлага эсвэл хязгаарлалтыг тусгаж болно. Жишээлбэл, итгэмжлэгдсэн ГОБ-д тодорхой гэрчилгээний бодлогын хувьд зөвхөн итгэмжлэгдэх боломжтой. Замын баталгаажуулалтын процедурын оролтуудаар энэхүү хязгаарлалтыг дэлгэрэнгүй тайлбарлах боломжтой.

Хэрэгжүүлэхдээ тодорхой итгэмжлэгдсэн талаас эхлэх хүчинтэй гэрчилгээжүүлэлтийн замыг цаашид хязгаарлахын тулд Хэсэг 6.1-д үзүүлсэн алгоритмыг сайжруулах БОЛОМЖТОЙ. Жишээлбэл, хэрэгжүүлэлт эхлүүлэх үе шатанд тодорхой итгэмжлэгдсэн талд замын уртын хязгаарлалт хэрэглэхийн тулд алгоритмыг өөрчилж болно, эсвэл аппликейшн нь зорилтот гэрчилгээнд өөр нэрийн маягт байхыг шаардаж болно, эсвэл аппликейшн нь тусгай өргөтгөлүүдэд шаардлага оруулж болно. Тиймээс 6.1-р хэсэгт үзүүлсэн замын баталгаажуулалтын алгоритм нь замыг хүчинтэй гэж үзэх хамгийн бага нөхцөлийг тодорхойлдог.

ГОБ нь итгэмжлэгдсэн талын мэдээллийг тодорхойлохын тулд өөрөө өөртөө гарын үсэг зурсан гэрчилгээг түгээдэг бол гэрчилгээний өргөтгөлүүдийг замын баталгаажуулалтад санал болгож буй оролтыг зааж өгөхөд ашиглаж болно. Жишээлбэл, энэхүү итгэмжлэгдсэн талаас эхэлсэн замуудыг зөвхөн тусгайлан тодорхойлсон бодлогын хувьд итгэмжлэх ёстойг харуулахын тулд бодлогын хязгаарлалтын өргөтгөлийг өөрөө өөртөө гарын үсэг зурсан гэрчилгээнд оруулж болно. Үүнтэй адилаар, энэ итгэмжлэгдсэн талаар эхэлсэн замууд нь зөвхөн заасан нэрийн орон зайд найдвартай байх ёстойг харуулахын тулд нэрийн хязгаарлалтын өргөтгөлийг оруулж болно. 6.1-р хэсэгт үзүүлсэн замын баталгаажуулалтын алгоритм нь итгэмжлэгдсэн талын мэдээллийг өөрөө

өөртөө гарын үсэг зурсан гэрчилгээнийх гэж үзэхгүй бөгөөд ийм гэрчилгээнд орсон нэмэлт мэдээллийг боловсруулах дүрмийг заагаагүй болно. Итгэмжлэгдсэн талын мэдээллийг тодорхойлохын тулд өөрөө өөртөө гарын үсэг зурсан гэрчилгээг ашигладаг хэрэгжүүлэлтүүд ийм мэдээллийг боловсруулах эсвэл орхих нь чөлөөтэй байдаг.

6.3. ХГЖ-ын баталгаажуулалт

Энэ хэсэгт ХГЖ нь гэрчилгээ олгогчийн ашигладаг хүчингүй болгох механизм гэвэл гэрчилгээг хүчингүй болгосон эсэхийг тодорхойлоход шаардлагатай алхмуудыг тайлбарласан болно. Энэ алгоритмыг хэрэгжүүлэхийн тулд ХГЖ-г дэмждэг хамаарах хэрэгжүүлэлтүүд шаардлагагүй, гэхдээ тэдгээр нь энэ профайлын дагуу гаргасан ХГЖ-г боловсруулахдаа энэхүү процедурын үр дүнд бий болох гадаад шинжтэй функциональ байдлаар тэнцүү байх ёстой. Аливаа алгоритмыг зөв үр дүнд хүрсэн тохиолдолд тодорхой хэрэгжүүлэлт ашиглаж болно.

Энэ алгоритм нь шаардлагатай бүх ХГЖ-г локал кэшэд хадгалах боломжтой байхаар авч үздэг. Тодруулбал, хэрэв ХГЖ-ын дараагийн шинэчлэлтийн хугацаа өнгөрсөн бол алгоритм нь одоогийн ХГЖ-г татаж аваад локал кэшэд байрлуулах боломжтой механизмыг авч үздэг.

Энэ алгоритм нь зам дахь гэрчилгээ бүрийн хувьд хийгдэх оролтын багц, төлөвийн хувьсагчийн багц, боловсруулах алхмуудыг тодорхойлдог. Алгоритмын гаралт нь гэрчилгээг хүчингүй болгох статус юм.

6.3.1. Хүчингүй болгох оролт

Хүчингүй болгох боловсруулалтыг дэмжихийн тулд алгоритм нь хоёр оролтыг шаарддаг:

A) гэрчилгээ: Алгоритм нь тухайн ХГЖ дээр гэрчилгээ байгаа эсэхийг тодорхойлохын тулд гэрчилгээний серийн дугаар болон олгогчийн нэрийг шаарддаг. Нийлүүлсэн гэрчилгээ нь ГОБ эсвэл эцсийн байгууллагатай холбоотой эсэхийг тодорхойлоход basicConstraints өргөтгөлийг ашигладаг. Хэрэв байгаа бол алгоритм нь хүчингүй болгох статусыг тодорхойлохын тулд cRLDistributionPoints болон freshestCRL өргөтгөлүүдийг ашигладаг.

B) use-deltas: Энэ логик оролт нь ХГЖ-д дельта ХГЖ-г хэрэглэж байгаа эсэхийг тодорхойлдог.

6.3.2. Эхлүүлэх болон хүчингүй болгох төлөвийн хувьсагчид

ХГЖ боловсруулалтыг дэмжихийн тулд алгоритм дараах төлөвийн хувьсагчдыг шаарддаг:

A) reasons_mask (шалтгааны_маск): Энэ хувьсагч нь одоогоор боловсруулсан ХГЖ болон дельта ХГЖ-аар дэмжигдсэн хүчингүй болгох шалтгаануудын багцыг агуулна. Багцын албан ёсны гишүүд нь тодорхойгүй утгуудыг хассан хүчингүй болгох шалтгаанууд байна: keyCompromise, cACompromise, affiliationChanged, орлуулсан, cessationOfoperation, certificateHold, privilegeWithdrawn, aACompromise. Бүх шалтгааны тусгай утгыг бүх албан ёсны гишүүдийн багцыг илэрхийлэхэд ашигладаг. Энэ хувьсагчийг хоосон багц байдлаар эхлүүлдэг.

B) cert_status: Энэ хувьсагч нь гэрчилгээний статусыг агуулна. Энэ хувьсагчийг дараах утгуудын аль нэгээр нь оноож болно: unspecified, keyCompromise, cACompromise, affiliationChanged, орлуулсан, StopOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn, aACompromise, UNREVOKED тусгай утга эсвэл UNTERMINED тусгай утга. Энэ хувьсагчийг UNREVOKED тусгай утгатайгаар эхлүүлдэг.

C) interim_reasons_mask (завсрын_шалтгаан_маск): Энэ нь одоогоор боловсруулж байгаа ХГЖ эсвэл delta ХГЖ-аар дэмжигдсэн хүчингүй болгох шалтгаануудын багцыг агуулна.

Тайлбар: Зарим орчинд бүх шалтгааны кодыг шалгах шаардлагагүй. Жишээлбэл, зарим орчин нь зөвхөн ГОБ-ын гэрчилгээнд зориулсан cACompromise болон keyCompromise-тэй холбоотой байдаг. Энэ алгоритм нь бүх шалтгааны кодыг шалгадаг. Шалгалтыг шалтгаан кодын дэд бүлэгт хязгаарлахад нэмэлт боловсруулалт болон төлөвийн хувьсагч шаардлагатай байж болно.

6.3.3. ХГЖ боловсруулалт

Гэрчилгээг цуцлаагүй гэж үзвэл энэ алгоритм эхэлнэ. Алгоритм нь нэг буюу хэд хэдэн ХГЖ-ын гэрчилгээний статусыг хүчингүй болгохоор тодорхойлох хүртэл эсвэл бүх шалтгааны кодыг хамрах хангалттай ХГЖ-ыг шалгах хүртэл ажиллана.

Гэрчилгээний ХГЖ түгээлтийн цэгийн өргөтгөл дэх түгээлтийн цэг (ТЦ) тус бүрийн хувьд локал ХГЖ кэш дэх харгалзах ХГЖ тус бүрийн хувьд ((шалтгаан_маск нь бүх шалтгаан биш) болон (cert_status нь UNREVOKED)) дараах үйлдлийг гүйцэтгэнэ:

A) Шаардлагатай бол бүрэн ХГЖ, дельта ХГЖ эсвэл хоёулангаар нь локал

ХГЖ кэшийг шинэчилнэ:

1) Хэрэв одоогийн цаг нь ХГЖ-ын дараагийн шинэчлэх талбарын утгаас хойш байвал дараахын аль нэгийг гүйцэтгэнэ:

   - Хэрэв use-deltas-ыг тохируулсан, мөн гэрчилгээ эсвэл ХГЖ нь хамгийн сүүлийн үеийн ХГЖ өргөтгөлийг агуулж байгаа бол одоогийн хугацаанаас хойших дараагийн шинэчлэлтийн утга бүхий дельта ХГЖ-аар 5.2.4-р хэсэгт заасны дагуу локал кэштэй ХГЖ-г шинэчлэхэд ашиглаж болно.

   - Локал ХГЖ кэшийг одоогийн бүрэн ХГЖ-аар шинэчилж, одоогийн цаг нь шинэ ХГЖ-ын дараагийн шинэчлэлтийн утгаас өмнө байгаа эсэхийг шалгаж, шинэ ХГЖ-аар үргэлжлүүлэн боловсруулна. Хэрэв use-deltas тохируулагдсан бөгөөд гэрчилгээ эсвэл ХГЖ нь хамгийн сүүлийн үеийн ХГЖ өргөтгөлийг агуулж байгаа бол 5.2.4-т заасны дагуу шинэ локал кэштэй бүрэн ХГЖ-г одоогийн дельта ХГЖ-аар шинэчилнэ.

2) Хэрэв одоогийн цаг нь дараагийн шинэчлэлтийн талбарын утгаас өмнө байвал user-deltas-г тохируулах, мөн гэрчилгээ эсвэл ХГЖ нь хамгийн сүүлийн үеийн ХГЖ өргөтгөлийг агуулж байгаа бол 5.2.4-р хэсэгт заасны дагуу локал кэштэй ХГЖ-г одоогийн дельта ХГЖ-г шинэчилнэ.

В) Бүрэн ХГЖ-ын олгогч болон хамрах хүрээг дараах байдлаар баталгаажуулна.

1) Хэрэв ТЦ нь cRLIssuer-г агуулж байгаа бол бүрэн ХГЖ-ын олгогчийн талбар нь ТЦ-ийн cRLIssuer-тэй нийцэж байгаа бөгөөд бүрэн ХГЖ нь шууд бус ХГЖ логик баталгаатай гаргах түгээлтийн цэгийн өргөтгөлийг агуулж байгаа эсэхийг шалгана. Үгүй бол ХГЖ олгогч нь гэрчилгээ олгогчтой нийцэж байгаа эсэхийг шалгана.

2) Хэрэв бүрэн ХГЖ нь олгох түгээх цэг (ОТЦ)- ийн ХГЖ өргөтгөлийг агуулсан байвал дараах зүйлийг шалгана:

   - Хэрэв түгээлтийн цэгийн нэр нь ОТЦ ХГЖ өргөтгөлд байгаа бөгөөд түгээх талбар нь ТЦ-д байгаа бол ОТЦ дахь нэрүүдийн аль нэг нь ТЦ-ын аль нэгтэй тохирч байгаа эсэхийг шалгана уу. Хэрэв түгээлтийн цэгийн нэр нь ОТЦ ХГЖ өргөтгөлд байгаа бөгөөд түгээх талбар нь ТЦ-ээс хасагдсан бол ОТЦ-ийн

нэрсийн аль нэг нь ТЦ-ын cRLIssuer талбарын аль нэгтэй таарч байгаа эсэхийг шалгана.

- Хэрэв onlyContainsUserCerts логик утга нь ОТЦ ХГЖ өргөтгөлд баталгаажсан бол баталгаажсан cA логик утгатай үндсэн хязгаарлалтын өргөтгөлийг гэрчилгээнд оруулсныг шалгана.
- Хэрэв onlyContainsCACerts логик утга нь ОТЦ ХГЖ өргөтгөлд баталгаажсан бол баталгаажсан cA логик утгатай үндсэн хязгаарлалтын өргөтгөлийг гэрчилгээнд оруулсныг шалгана.
- onlyContainsAttributeCerts логик утга батлагдаагүй эсэхийг шалгана.

C) Хэрэв user-deltas-ыг тохируулсан бол дельта ХГЖ-ын олгогч болон хамрах хүрээг дараах байдлаар шалгана:

1) Дельта ХГЖ олгогч нь бүрэн ХГЖ олгогчтой нийцэж байгаа эсэхийг шалгана.

2) Хэрэв бүрэн ХГЖ нь олгох түгээх цэгийн (ОТЦ) ХГЖ өргөтгөлийг агуулсан бол дельта ХГЖ нь тохирох ОТЦ ХГЖ өргөтгөлтэй эсэхийг шалгана. Хэрэв бүрэн ХГЖ нь ОТЦ ХГЖ өргөтгөлийг орхигдуулсан бол дельта ХГЖ нь ОТЦ ХГЖ өргөтгөлийг орхигдуулсан эсэхийг шалгана.

3) Дельта ХГЖ эрх бүхий түлхүүр адилтгагчийн өргөтгөл нь бүрэн ХГЖ эрх бүхий түлхүүр адилтгагчийн өргөтгөлтэй нийцэж байгаа эсэхийг шалгана.

D) Энэ ХГЖ-ын interim_reasons_mask (завсрын_шалтгаан_маск)-ийг дараах байдлаар тооцоолно:

1) Хэрэв олгох түгээх цэгийн (ОТЦ) ХГЖ өргөтгөл байгаа бөгөөд үүнд зөвхөн onlySomeReasons болон ТЦ-д шалтгаан багтсан бол interim_reasons_mask (завсрын_шалтгаан_маск)-ийг ТЦ болон ОТЦ ХГЖ өргөтгөл дэх onlySomeReasons болон ТЦ-д шалтгаануудын огтлолцолд тохируулна.

2) Хэрэв ОТЦ ХГЖ өргөтгөл нь onlySomeReasons-ыг агуулж байгаа боловч ТЦ нь шалтгаануудыг орхигдуулсан бол ОТЦ ХГЖ өргөтгөлийн onlySomeReasons утгаар interim_reasons_mask-ийг тохируулна.

3) Хэрэв ОТЦ ХГЖ өргөтгөл байхгүй эсвэл орхигдуулсан байгаа боловч ТЦ нь шалтгаануудыг оруулсан бол ОТЦ ХГЖ өргөтгөлийн утгаар

interim_reasons_mask-ийг тохируулна.

4) Хэрэв ОТЦ ХГЖ өргөтгөл нь байхгүй эсвэл onlySomeReasons-ыг орхигдуулсан бөгөөд ТЦ нь шалтгаануудыг оруулсан бол all-reasons тусгай утгуудад interim_reasons_mask-ийг тохируулна.

E) interim_reasons_mask (Завсрын_шалтгаан_маск) нь шалтгаан_маск-д ороогүй нэг буюу хэд хэдэн шалтгааныг агуулсан эсэхийг шалгана.

F) Бүрэн ХГЖ олгогчийн баталгаажуулалтын замыг авч баталгаажуулах. Баталгаажуулалтын замын итгэмжлэгдсэн тал нь зорилтот гэрчилгээг баталгаажуулахад ашигладаг итгэмжлэгдсэн талтай ижил байх ёстой. Хэрэв ХГЖ олгогчийн гэрчилгээнд түлхүүрийн хэрэглээний өргөтгөл байгаа бол cRLSign бит тохируулагдсан эсэхийг шалгана.

G) (f) алхамд баталгаажуулсан нийтийн түлхүүрийг ашиглан бүрэн ХГЖ дээрх гарын үсгийг баталгаажуулна.

H) Хэрэв user-deltas тохируулагдсан бол (f) алхамд баталгаажуулсан нийтийн түлхүүрийг ашиглан дельта ХГЖ дээрх гарын үсгийг баталгаажуулна.

I) Хэрэв user-deltas тохируулагдсан бол дельта ХГЖ дээрх гэрчилгээг хайна. Хэрэв хэсэг 5.3.3-т заасны дагуу гэрчилгээ олгогч болон серийн дугаартай таарч байгаа бичлэг олдвол cert_status хувьсагчийг доорх шалтгаанаар тохируулна.

1) Хэрэв шалтгаан кодын ХГЖ бичлэгийн өргөтгөл байгаа бол cert_status хувьсагчийг шалтгаан кодын ХГЖ бичлэгийн өргөтгөлийн утгаар тохируулна.

2) Хэрэв шалтгаан код ХГЖ бичлэгийн өргөтгөл байхгүй бол cert_status хувьсагчийг тодорхойгүй утгаар тохируулна.

J) Хэрэв (cert_status нь removeFromCRL) бол бүрэн ХГЖ дээрээс гэрчилгээг хайж олно. Хэсэг 5.3.3-т заасны дагуу гэрчилгээ олгогч болон серийн дугаартай таарч байгаа бичилт олдвол (i) алхамд тайлбарласны дагуу cert_status хувьсагчийг заасан шалтгаанаар тохируулна.

K) Хэрэв (cert_status бол removeFromCRL) бол cert_status-г UNREVOKED болгож тохируулна.

L) Шалтгаан_маск төлөвийн хувьсагчийг өмнөх утга болон завсрын_шалтгаан_маск төлөвийн хувьсагчийн нэгтгэл болгож тохируулна.

Хэрэв ((reasons_mask нь all-reasons) ЭСВЭЛ (cert_status нь UNREVOKED биш)) бол хүчингүй болгох статус тодорхойлогдсон тул cert_status-ыг буцаана.

Хэрэв хүчингүй болгох статус тодорхойлогдоогүй бол түгээлтийн цэгт заагаагүй боловч гэрчилгээ олгогчоос олгосон боломжтой ХГЖ-аар дээрх үйлдлийг давтан хийнэ. Ийм ХГЖ-г боловсруулахын тулд орхигдуулсан шалтгаан болон cRLIssuer талбаруудыг хоёуланг, болон гэрчилгээ олгогчийн түгээлтийн цэгийн нэрийг нь агуулсан ТЦ-г авч үзнэ. Өөрөөр хэлбэл, fullName дэх нэрсийн дарааллыг гэрчилгээ олгогчийн талбар болон гэрчилгээ олгогчийн AltName өргөтгөлөөс үүсгэнэ. Ийм ХГЖ-г боловсруулсны дараа, хэрэв хүчингүй болгох статус хараахан тогтоогдоогүй байгаа бол cert_status ТОДОРХОЙГҮЙ гэж буцаана.

7. Олон улсын нэрсэд зориулсан боловсруулах дүрмүүд

Олон тооны гэрчилгээ болон ХГЖ-ийн талбарууд, өргөтгөлүүд дэх олон улсын чанартай нэрстэй таарч болно. Үүнд онцлох нэрс, олон улсын домэйн нэрс, цахим шуудангийн хаяг, олон улсын нөөцийн адилтгагчид (ОУНА) орно.

Ийм нэрийг хадгалах, харьцуулах, танилцуулах нь онцгой анхаарал шаарддаг. Зарим тэмдэгтүүдийг олон янзаар шифрлэж болно.

Ижил нэрсийг олон тооны шифирлэлтэнд (жишээ нь, ASCII эсвэл UTF8) төлөөлж болно.

Энэ бүлэг нь эдгээр нэрийн маягт бүрийг хадгалах эсвэл харьцуулахад зориулсан нийцлийн шаардлагыг тогтооно.

Эдгээр нэрийн маягтуудын заримд нь танилцуулгын талаарх мэдээллийн удирдамжийг өгсөн болно.

7.1. Онцлох нэрс дэх олон улсын нэрс

Онцлох нэрс дэх олон улсын нэрсийн төлөөллийг 4.1.2.4 дэх олгогчийн нэр, 4.1.2.6 дэх субъектийн нэр хэсгүүдэд тусгасан болно.

Стандарт нэрийн атрибутууд, жишээ нь нийтлэг нэр, нь Стандарт нэрс нь төрөл бүрийн хэлний шифрлэлтээр дамжуулан олон улсын нэрсийг дэмждэг DirectoryString төрлийг ашигладаг.

Тохиромжтой хэрэгжүүлэлт нь UTF8String болон PrintableString-г ЗААВАЛ дэмжинэ.

RFC 3280 нь UTF8String-д кодлогдсон атрибутын утгуудын зөвхөн хоёртын харьцуулалтыг шаарддаг. Гэсэн хэдий ч, энэ тодорхойлолт нь харьцуулалтыг илүү өргөн хүрээнд авч үзэхийг шаарддаг.

Хэрэгжүүлэлтэд TeletexString, BMPString, эсвэл UniversalString ашиглан кодлогдсон гэрчилгээ болон ХГЖ-уудтай тулгарч болно. Гэхдээ эдгээрийг

дэмжих нь ЗААВАЛ биш юм.

Тохиромжтой хэрэгжүүлэлтүүд нь PrintableString эсвэл UTF8String-д аль алинд нь кодлогдсон онцлох нэрийн атрибутуудын харьцуулалтад зориулсан үндэс болгон [RFC4518]-д заасны дагуу LDAP StringPrep профайл (зайг ач холбогдолгүй ашиглах багтана)-ыг ЗААВАЛ ашиглана.

Тохиромжтой хэрэгжүүлэлтүүд caseIgnoreMatch ашиглан нэрийн харьцуулалтыг ЗААВАЛ дэмжинэ.

Атрибутын төрлүүдэд зориулсан дэмжлэг буюу бусад тэгш байдлыг тохирох дүрмүүдийг хэрэглэх нь нэмэлт юм.

CaseIgnoreMatch тохирох дүрмийг ашиглан нэрсийг харьцуулахын өмнө тохирох хэрэгжүүлэлтүүд нь дараах тодруулгын хамт төрөл DirectoryString-ийн атрибут тус бүрд [RFC4518]-д тайлбарласан six-step string бэлтгэх алгоритмыг ЗААВАЛ гүйцэтгэнэ.

* 2-р алхамд, Газрын зураг, зураглал [RFC3454]-ийн Хавсралт B.2-т заасны дагуу хавтас нугалахыг оруулах ёстой.

* 6-р алхамд, Ач холбогдолгүй тэмдэгтийг арилгах нь [RFC4518]-ийн Ач холбогдолгүй орон зайг зохицуулах, 2.6.1-д заасны дагуу хоосон зай шахалтыг гүйцэтгэдэг.

Мөр бэлтгэх алгоритмыг гүйцэтгэх үед атрибутуудыг хадгалсан утгууд гэж ЗААВАЛ засна.

domainComponent атрибутуудын харьцуулалтууд Бүлэг 7.3-т заасны дагуу ЗААВАЛ гүйцэтгэгдэнэ.

Хэрвээ атрибутын төрлүүд ижил ба мөр бэлтгэх алгоритмтай боловсруулсны дараа атрибутуудын утгууд нь яг таарч байвал хоёр нэрлэх атрибут таарна.

Хамааралтай ялгагч нэр (ХЯН)1 ба ХЯН2 хоёр онцлох нэрс нь ижил тооны нэрлэх атрибуттай бөгөөд ХЯН1 дэх нэрлэх атрибут бүрд ХЯН2-д тохирох нэрлэх атрибут байвал таарна.

Хэрэв ижил тооны ХЯН-тэй бол ЯН1 ба ЯН2 хоёр онцлох нэр таарч, ЯН1-д байгаа ХЯН бүрийн хувьд ЯН2-д тохирох ХЯН байх ба тохирох ХЯН-ууд нь хоёуланд нь ижил дарааллаар харагдана.

Хэрэв ЯН1 нь ЯН2 шиг олон тооны ХЯН-уудыг наанадаж агуулж байвал онцлох нэр ЯН1 нь онцлох нэр ЯН2-оор тодорхойлогдсон дэд мод дотор байна. Мөн ЯН1 дэх ардах ХЯН-уудыг үл тоомсорлосон үед ЯН1 ба ЯН2 –ууд нь таарна.

7.2. GeneralName дэх олон улсын домэйн нэрс

Олон улсын домэйн нэр (ОУДН) нь subjectAltName болон issuerAltName өргөтгөл, нэрийн хязгаарлалтын өргөтгөл, байгууллагын мэдээллийн хандалтын өргөтгөл, субъектийн мэдээллийн хандалтын өргөтгөл,

ХГЖ түгээх цэгүүдийн өргөтгөл, олгож байгаа түгээлтийн цэгийн өргөтгөл зэрэгт гэрчилгээ болон ХГЖ-д багтаж болно.

Эдгээр өргөтгөл бүр нь GeneralName төрлийг ашигладаг; GeneralName - ийн нэг сонголт нь dNSName талбар бөгөөд IA5String төрөл гэж тодорхойлогддог.

IA5String нь ASCII тэмдэгтүүдийн багцаар хязгаарлагддаг.

Олон улсын домэйн нэрийг одоогийн бүтцэд нийцүүлэхийн тулд тохиромжтой хэрэгжүүлэлт нь dNSName талбарт хадгалахын өмнө RFC 3490-ийн 4-р бүлэгт заасан ASCII Compatible Encoding (ACE) формат руу олон улсын домэйн нэрийг ЗААВАЛ хөрвүүлнэ.

Тодруулбал, тохиромжтой хэрэгжүүлэлт нь RFC 3490-ийн 4-р бүлэгт заасан хувиргах үйлдлийг дараах тодруулгын хамт ЗААВАЛ гүйцэтгэнэ.

* 1-р алхамд домэйн нэрийг "хадгалагдсан мөр" гэж үзсэн байх ХЭРЭГТЭЙ. Өөрөөр хэлбэл, AllowUnassigned тугийг тохируулах ХЭРЭГГҮЙ;

* 3-р алхамд "UseSTD3ASCIIRules" нэртэй тугийг тохируулна;

* 4-р алхамд шошго бүрийг "ToASCII" үйлдлээр боловсруулна;

* 5-р алхамд бүх шошго тусгаарлагчийг U+002E (full stop) болгож өөрчил.

DNS нэрсийг тэнцүүлэн харьцуулахдаа тохиромжтой хэрэгжүүлэлтүүд нь бүрэн DNS нэр дээр (case-insensitive) том жижиг үсгээс үл хамааран яг таарч байхаар ЗААВАЛ гүйцэтгэнэ.

Нэрсний хязгаарлалтыг үнэлэхдээ, тохиромжтой хэрэгжүүлэлтүүд нь шошго тус бүрээр том жижиг үсгээс үл хамааран яг таарч байхаар ЗААВАЛ гүйцэтгэнэ.

4.2.1.10-д тэмдэглэсэнчлэн аливаа DNS нэрийг заасан нэрийн дэд модон дотор оруулан хязгаарлалтыг авч үздэг шиг шошгуудыг өгөгдсөн домэйн нэрийн зүүн гар талд нэмэх байдлаар хязгаарлаж болно.

Хэрэгжүүлэлтүүд нь дэлгэцэд харуулахын өмнө ОУДН-уудыг Юникод руу хөрвүүлэх ёстой.

Тодруулбал, тохиромжтой хэрэгжүүлэлт нь RFC 3490-ийн 4-р бүлэгт заасан хувиргах үйлдлийг дараах тодруулгын хамт гүйцэтгэх ёстой.

* 1-р алхамд домэйн нэрийг "хадгалагдсан мөр" гэж үзсэн байх ХЭРЭГТЭЙ. Өөрөөр хэлбэл, AllowUnassigned тугийг тохируулах ХЭРЭГГҮЙ;

* 3-р алхамд "UseSTD3ASCIIRules" нэртэй тугийг тохируулна;

* 4-р алхамд шошго бүрийг "ToUnicode" үйлдлээр боловсруулна;

* 5-р алхмыг алгасна.

Тайлбар: Хэрэгжүүлэлтүүд нь ОУДН-д зориулан зайны шаардлагуудыг нэмэгдүүлэхийг ЗААВАЛ зөвшөөрнө.

ОУДН ACE шошго нь "xn--" дөрвөн нэмэлт тэмдэгтээр эхлэх бөгөөд

нэг олон улсын тэмдэгтийг таван ASCII тэмдэгтүүд заахтай адил таваас илүүг шаардаж болно.

7.3. Онцлох нэрс дэх олон улсын домэйн нэрс

Домэйн нэрсийг мөн субъект талбар, олгогч талбар, subjectAltName өргөтгөл эсвэл issuerAltName өргөтгөл дэх домэйн бүрэлдэхүүн хэсгүүдийг ашиглан онцолсон нэрээр төлөөлүүлж болно.

GeneralName төрлийн dNSName-ийн нэгэн адил энэ атрибутын утгыг IA5String гэж тодорхойлсон.

DomainComponent атрибут бүр нь ганц шошгыг илэрхийлдэг.

Онцлох нэрэнд ОУДН-аас шошгыг илэрхийлэхийн тулд хэрэгжүүлэлт нь RFC 3490-ийн 4.1-д заасан "ToASCII" шошгын хувиргалтыг ЗААВАЛ гүйцэтгэнэ.

Шошгыг "хадгалагдсан мөр" гэж үзсэн байх ХЭРЭГТЭЙ. Өөрөөр хэлбэл, AllowUnassigned тугийг тохируулах ХЭРЭГГҮЙ;

Тохиромжтой хэрэгжүүлэлт нь Бүлэг 7.2-т тодорхойлсон шиг онцлох нэрс дэх domainComponent атрибутуудыг харьцуулж байгаа үед том жижиг үсгээс үл хамааран яг таарч байхаар гүйцэтгэх хэрэгтэй.

Хэрэгжүүлэлтүүд нь дэлгэцэд харуулахын өмнө ACE шошгыг Юникод болгон хөрвүүлэх ёстой. Тодруулбал тохиромжтой хэрэгжүүлэлтүүд нь нэрийг дэлгэцэд харуулахаас өмнө ACE шошго бүр дээр Бүлэг 7.2-т тодорхойлсны дагуу "ToUnicode" хувиргах үйлдлийг гүйцэтгэх ёстой.

7.4. Олон улсын нөөцийн адилтгагч

Олон улсын нөөцийн адилтгагч (ОУНА) нь нөөцийн нэгдсэн адилтгагч (ННА)-ийн олон улсын нэмэлт юм.

ОУНА нь Юникод тэмдэгтүүдийн дараалал, харин ННА нь ASCII тэмдэгтийн багцалсан тэмдэгтүүдийн дараалал юм.

[RFC3987] нь ОУНА-аас ННА-руу зураглалыг тодорхойлдог.

Хэдийгээр ОУНА нь аливаа гэрчилгээний талбар эсвэл өргөтгөлүүдэд шууд шифрлэгдээгүй ч тэдгээрийн зураглагдсан ННА-г гэрчилгээ болон ХГЖ-д багтааж болно.

ННА- ууд нь subjectAltName болон issuerAltName өргөтгөлүүд, нэрийн хязгаарлалтын өргөтгөл, байгууллагын мэдээллийн хандалтын өргөтгөл, субъектийн мэдээллийн хандалтын өргөтгөл, ХГЖ-ийн түгээх цэгүүдийн өргөтгөлүүдэд гарч ирж болно.

Эдгээр өргөтгөл бүр нь GeneralName төрлийг ашигладаг; ННА нь GeneralName дэх uniformResourceIdentifier талбарт шифрлэгдэх бөгөөд IA5String төрөл гэж тодорхойлогддог.

Одоогийн бүтцэд ОУНА-г байрлуулахад, тохиромжтой хэрэгжүүлэлт нь [RFC3987]-ийн 3.1-д заасны дагуу ОУНА-г ННА-д дараах тодруулгын хамт ЗААВАЛ буулгана.

* 1-р алхамд b хувилбарт заасан NFC-ийн дагуу хэвийн болгох анхны ОУЧТТ форматаас UCS тэмдэгтийн дарааллыг үүсгэнэ (NFC-ийн дагуу хэвийн болгох);

* 1-р алхмын гаралтыг ашиглан 2-р алхмыг гүйцэтгэнэ.

Хэрэгжилтүүд 2-р алхмыг хийхээс өмнө ireg-name бүрэлдэхүүнийг хөрвүүлэх БОЛОХГҮЙ.

URI-г харьцуулахаас өмнө тохирох хэрэгжүүлэлтүүд нь [RFC3987]-д тайлбарласан синтакс болон схемд суурилсан хэвийн болгох аргуудыг хослуулан гүйцэтгэх ёстой.

Тохиромжтой хэрэгжүүлэлтүүд нь URI-г дараах байдлаар харьцуулахаар бэлтгэсэн байх ёстой.

* Алхам 1: Хэрэв ОУЧТТ нь IDN ашиглахыг зөвшөөрдөг бол дээрх нэрсийг 7.2-р хэсэгт заасны дагуу ASCII нийцтэй кодчилол руу хөрвүүлэх ЗААВАЛ хэрэгтэй.

* Алхам 2: [RFC3987]-ийн 5.3.2.1-д тайлбарласны дагуу схем болон хостыг жижиг үсгээр хэвийн болгосон.

* Алхам 3: [RFC3987]-ийн 5.3.2.3-т заасны дагуу хувийн кодчиллыг хэвийн болгох.

* Алхам 4: [RFC3987]-ийн 5.3.2.4-т заасны дагуу замын сегментийг хэвийн болгох.

* Алхам 5: Хэрэв хүлээн зөвшөөрөгдсөн бол хэрэгжилт нь [RFC3987]-ийн 5.3.3-т заасны дагуу схемд суурилсан хэвийн болгох ёстой.

Тохиромжтой хэрэгжүүлэлтүүд нь ldap, http, https, ftp гэсэн схемүүдийн схемд суурилсан нормчлохыг хүлээн зөвшөөрч гүйцэтгэх ёстой. Хэрэв схемийг танихгүй бол 5-р алхмыг орхигдуулна.

URI-г дүйцүүлэх үүднээс харьцуулахдаа нийцэж буй хэрэгжүүлэлт нь том жижиг үсгээр яг таарч тохирно.

Хэрэгжүүлэлтүүд нь харуулахын өмнө URI-г Юникод руу хөрвүүлэх ёстой. Тодруулбал, нийцсэн хэрэгжүүлэлт нь [RFC3987]-ийн 3.2-т заасан хувиргах үйлдлийг гүйцэтгэх ёстой.

7.5. Олон улсын цахим шуудангийн хаяглалт

SubjectAltName болон issuerAltName өргөтгөл, нэрийн хязгаарлалтын өргөтгөл, эрх мэдлийн мэдээллийн хандалтын өргөтгөл, субъект мэдээллийн хандалтын өргөтгөл, гаргах түгээх цэгийн өргөтгөл, ХГЖ түгээх цэгийн өргөтгөл зэрэгт цахим шуудангийн хаягуудыг гэрчилгээ болон ХГЖ-д оруулж болно.

Эдгээр өргөтгөл бүр нь GeneralName бүтцийг ашигладаг; GeneralName нь rfc822Name сонголтыг агуулдаг бөгөөд энэ нь IA5String төрөл гэж тодорхойлогддог.

Одоогийн бүтцийг ашиглан олон улсын домэйн нэртэй и-мэйл хаягуудыг байрлуулахын тулд нийцсэн хэрэгжүүлэлтүүд нь хаягуудыг ASCII дүрслэл болгон хувиргах ёстой.

Хост-хэсэг (мэйл хайрцгийн домэйн) олон улсын нэр агуулсан бол 7.2-р хэсэгт заасны дагуу домэйн нэрийг IDN-ээс ASCII нийцтэй кодчилол (ACE) формат руу хөрвүүлэх ёстой.

Дараах тохиолдолд хоёр и-мэйл хаяг таарч байна:

1) Нэр бүрийн орон нутгийн хэсэг нь яг таарч байна, БА
2) нэр тус бүрийн хост хэсэг нь том жижиг жижиг ASCII харьцуулалтыг ашиглан таарч байна.

Хэрэгжилтүүд нь харуулахын өмнө эдгээр өргөтгөлүүдэд заасан олон улсын чанартай и-мэйл хаягуудын хост хэсгийг Юникод руу хөрвүүлэх ёстой.

Тохиромжтой хэрэгжүүлэлтүүд нь 7.2-р хэсэгт тайлбарласны дагуу шуудангийн хайрцгийн хост хэсгийг хөрвүүлэх ёстой.

8. Аюулгүй байдлын хязгаарлалтууд

Энэхүү тодорхойлолтын ихэнх нь гэрчилгээ болон ХГЖ-ийн хэлбэр, агуулгад зориулагдсан болно.

Гэрчилгээ болон ХГЖ нь дижитал гарын үсэг зурсан тул бүрэн бүтэн байдлын нэмэлт үйлчилгээ шаардлагагүй.

Гэрчилгээ болон ХГЖ-ийн аль алиныг нь нууцлах шаардлагагүй бөгөөд гэрчилгээ болон ХГЖ-д хязгаарлалтгүй, нэргүй хандах нь аюулгүй байдалд ямар ч нөлөө үзүүлэхгүй.

Гэсэн хэдий ч, энэ тодорхойлолтын хамрах хүрээнээс гадуурх аюулгүй байдлын хүчин зүйлүүд нь гэрчилгээ хэрэглэгчдэд олгосон баталгаанд нөлөөлнө.

Энэ хэсэгт хэрэгжүүлэгчид, администраторууд болон хэрэглэгчдийн анхаарах ёстой чухал асуудлуудыг онцолсон болно.

Субъектийн таних тэмдгийг нийтийн түлхүүртэй нь холбохыг баталгаажуулахын тулд ГОБ болон ББ-ын гүйцэтгэсэн процедур нь гэрчилгээнд байршуулах ёстой баталгаанд ихээхэн нөлөөлдөг.

Итгэмжлэгдсэн талууд ГОБ-ийн баталгаажуулалтын практик мэдэгдлийг хянаж үзэхийг хүсэж болно. Энэ нь бусад ГОБ-д гэрчилгээ олгоход онцгой чухал юм.

Гарын үсэг болон бусад зорилгоор нэг түлхүүрийн хослолыг ашиглахыг хатуу хориглоно.

Гарын үсэг болон түлхүүрийн удирдлагад тус тусад нь хос түлхүүр ашиглах нь хэрэглэгчдэд хэд хэдэн давуу талыг өгдөг.

Гарын үсгийн түлхүүрийг алдах эсвэл задруулахтай холбоотой үр дагавар нь удирдлагын түлхүүрийг алдах эсвэл задруулахаас ялгаатай.

Тусдаа түлхүүрүүдийг ашиглах нь тэнцвэртэй, уян хатан хариу үйлдэл үзүүлэх боломжийг олгодог.

Үүний нэгэн адил, түлхүүр хос бүрийн хүчинтэй байх хугацаа эсвэл түлхүүрийн урт нь зарим хэрэглээний орчинд тохиромжтой байж болно.

Харамсалтай нь зарим хуучин программууд (жишээ нь, Secure Sockets Layer (SSL)) гарын үсэг болон түлхүүрийн удирдлагад нэг түлхүүрийн хослол ашигладаг.

Хувийн түлхүүрүүдийн хамгаалалт нь аюулгүй байдлын чухал хүчин зүйл юм.

Хэрэглэгчид хувийн түлхүүрээ хамгаалаагүй тохиолдолд халдагчид өөрсдийнхөө дүрд хувирах эсвэл хувийн мэдээллээ тайлах боломжийг олгоно.

Томоохон хэмжээгээр, ГОБ- ийн хувийн гарын үсэг зурах түлхүүрийг эвдэх нь сүйрлийн үр дагаварт хүргэж болзошгүй юм.

Хэрэв халдагч хувийн түлхүүрийг анзааралгүй олж авбал халдагчид хуурамч

гэрчилгээ болон ХГЖ гаргаж болзошгүй.

Хуурамч гэрчилгээ, ХГЖ байгаа нь системд итгэх итгэлийг бууруулна.

Хэрэв иймэвдрэл илэрсэн бол эвдэрсэн ГОБ- д олгосон бүх гэрчилгээг хүчингүй болгож, түүний хэрэглэгчид болон бусад ГОБ- ын хэрэглэгчдийн хооронд үйлчилгээ үзүүлэхээс сэргийлнэ.

Ийм буулт хийсний дараа сэргээн босгох нь асуудалтай тул ГОБ- д ийм тохиолдлоос зайлсхийхийн тулд хүчирхэг техникийн арга хэмжээ (жишээ нь, хөндлөнгийн оролцоонд тэсвэртэй криптограф модулиуд) болон зохих менежментийн журам (жишээ нь, үүрэг хуваах) хослуулан хэрэгжүүлэхийг зөвлөж байна.

ГОБ- ийн хувийн гарын үсэг алдагдах нь бас асуудалтай байж болно.

ГОБ нь ХГЖ үүсгэх эсвэл ердийн түлхүүр эргүүлэх боломжгүй. ГОБ- ууд гарын үсэг зурах түлхүүрүүдийг найдвартай нөөцлөх ХЭРЭГТЭЙ.

Түлхүүр нөөцлөх процедурын аюулгүй байдал нь гол буултаас зайлсхийх чухал хүчин зүйл юм.

Хүчингүй болгох мэдээллийн хүртээмж, шинэлэг байдал нь гэрчилгээнд байршуулах ёстой баталгааны зэрэгт нөлөөлдөг.

Гэрчилгээний хүчинтэй хугацаа нь аяндаа дуусдаг хэдий ч түүний байгалийн амьдралын туршид субъект болон нийтийн түлхүүрийн хоорондох холболтыг үгүйсгэдэг үйл явдал тохиолдож болно.

Хэрэв хүчингүй болгох тухай мэдээлэл цаг тухайд нь байхгүй эсвэл боломжгүй бол заавал дагаж мөрдөхтэй холбоотой баталгаа тодорхой буурна.

Найдвартай талууд ХГЖ- д гарч болох чухал өргөтгөл бүрийг боловсруулах боломжгүй байж магадгүй.

ГОБ нь зөвхөн чухал өргөтгөлүүдийг агуулсан ХГЖ-ээр дамжуулан хүчингүй болгох мэдээллийг нээлттэй болгохдоо онцгой анхаарал тавих ёстой, ялангуяа эдгээр өргөтгөлүүдийг дэмжих нь энэ профайлд заагаагүй тохиолдолд.

Жишээлбэл, хэрэв хүчингүй болгох мэдээллийг дельта ХГЖ болон бүтэн ХГЖ-ийн хослолыг ашиглан нийлүүлж, дельта ХГЖ- ийг бүрэн ХГЖ- ээс илүү олон удаа гаргадаг бол дельта ХГЖ боловсруулахтай холбоотой чухал өргөтгөлүүдийг зохицуулж чадахгүй байгаа найдах талууд үүнийг хийх боломжгүй болно. хамгийн сүүлийн хүчингүй болгох мэдээллийг авах.

Өөрөөр хэлбэл, дельта ХГЖ гарах бүрд бүрэн ХГЖ-г гаргадаг бол бүх итгэмжлэгдсэн талуудад цаг тухайд нь хүчингүй болгох мэдээллийг авах

боломжтой.

Үүний нэгэн адил, хүчингүй болгох шалгалтыг орхигдуулсан 6-р бүлэгт тодорхойлсон баталгаажуулалтын замыг баталгаажуулах механизмын хэрэгжилт нь үүнийг дэмждэгтэй харьцуулахад бага баталгаа өгдөг.

Баталгаажуулалтын замыг баталгаажуулах алгоритм нь нэг буюу хэд хэдэн итгэмжлэгдсэн ГОБ-ийн талаарх нийтийн түлхүүрүүдийн (болон бусад мэдээлэл) тодорхой мэдлэгээс хамаарна.

ГОБ-д итгэх шийдвэр нь эцсийн дүндээ гэрчилгээ олгох итгэлийг тодорхойлдог чухал шийдвэр юм.

Итгэмжлэгдсэн ГОБ нийтийн түлхүүрүүдийг баталгаажуулсан түгээлт (ихэвчлэн "өөрөө гарын үсэг зурсан" гэрчилгээ хэлбэрээр) нь энэ тодорхойлолтын хамрах хүрээнээс гадуур, аюулгүй байдлын чухал үйл явц юм.

Нэмж дурдахад, итгэмжлэгдсэн ГОБ-д түлхүүр эвдрэл эсвэл ГОБ алдаа гарсан тохиолдолд хэрэглэгч зам баталгаажуулалтын горимд өгсөн мэдээллийг өөрчлөх шаардлагатай болно.

Хэт олон итгэмжлэгдсэн ГОБ-г сонгох нь итгэмжлэгдсэн ГОБ мэдээллийг хадгалахад хэцүү болгодог.

Нөгөө талаас, зөвхөн нэг итгэмжлэгдсэн ГОБ-г сонгох нь хэрэглэгчдийг хаалттай хэрэглэгчдийн нийгэмлэгт хязгаарлаж болзошгүй юм.

Гэрчилгээг боловсруулдаг хэрэгжилтийн чанар нь баталгааны зэрэгт нөлөөлдөг.

6-р хэсэгт тайлбарласан замын баталгаажуулалтын алгоритм нь итгэмжлэгдсэн ГОБ мэдээллийн бүрэн бүтэн байдал, ялангуяа итгэмжлэгдсэн ГОБ-тай холбоотой нийтийн түлхүүрүүдийн бүрэн бүтэн байдалд тулгуурладаг.

Халдагчид хувийн түлхүүртэй нийтийн түлхүүрүүдийг орлуулснаар халдагчид хэрэглэгчийг хууран мэхэлж, хуурамч гэрчилгээ авах боломжтой.

Түлхүүр болон гэрчилгээний субъект хоорондын холболт нь гарын үсэг үүсгэхэд ашигладаг криптограф модулийн хэрэгжилт болон алгоритмаас илүү хүчтэй байж болохгүй.

Түлхүүрийн богино урт эсвэл сул хэш алгоритм нь гэрчилгээний хэрэглээг хязгаарлах болно.

ГОБ- г криптологийн дэвшлийг тэмдэглэхийг зөвлөж байна, ингэснээр тэд хүчтэй криптографийн арга техникийг ашиглах боломжтой болно.

Нэмж дурдахад, ГОБ нь сул гарын үсэг үүсгэдэг ГОБ эсвэл эцсийн байгууллагуудад гэрчилгээ олгохоос татгалзах ХЭРЭГТЭЙ.

Нэрийн харьцуулах дүрмийг үл нийцүүлэх нь хүчингүй X.509 гэрчилгээний замыг хүлээн зөвшөөрөх эсвэл хүчинтэйг нь татгалзахад хүргэж болзошгүй.

X.500 цуврал техникийн үзүүлэлтүүд нь том жижиг үсэг, тэмдэгтийн багц, олон тэмдэгтийн цагаан зайны дэд тэмдэгт, эхний болон хойно байгаа цагаан зай зэргийг харгалзахгүйгээр мөрүүдийг харьцуулах шаардлагатай нэрсийг харьцуулах дүрмийг тодорхойлдог.

Энэхүү тодорхойлолт нь эдгээр шаардлагыг зөөлрүүлж, хамгийн багадаа хоёртын харьцуулалтыг дэмжихийг шаарддаг.

ГОБ нь ГОБ гэрчилгээний сэдвийн талбар дахь ялгагдах нэрийг тухайн ГОБ-аас олгосон гэрчилгээний гаргагчийн талбар дахь ялгасан нэртэй ижил кодлох ЗААВАЛ.

Хэрэв ГОБ-ууд өөр кодчилол ашигладаг бол хэрэгжүүлэлтүүд энэ гэрчилгээг агуулсан замуудын нэрийн хэлхээг таньж чадахгүй байж магадгүй.

Үүний үр дүнд хүчинтэй замуудаас татгалзаж болно.

Нэмж хэлэхэд, онцлох нэрэнд зориулсан нэрийн хязгаарлалтыг субъект талбар эсвэл subjectAltName өргөтгөл дэх кодчилолтой яг адилхан зааж өгөх ёстой.

Үгүй бол хасагдсан дэд мод гэж тодорхойлсон нэрийн хязгаарлалтууд таарахгүй бөгөөд хүчингүй замуудыг хүлээн авах ба зөвшөөрөгдсөн Дэд мод гэж илэрхийлсэн нэрийн хязгаарлалтууд таарахгүй бөгөөд хүчинтэй замуудаас татгалзах болно.

Хүчингүй замыг хүлээн зөвшөөрөхөөс зайлсхийхийн тулд ГОБ-ууд аль болох боломжтой бол зөвшөөрөгдсөн дэд мод гэж ялгагдах нэрийн хязгаарлалтыг зааж өгөх ХЭРЭГТЭЙ.

Ерөнхийдөө nameConstraints өргөтгөлийг нэг нэрийн маягтыг (жишээ нь, DNS нэр) хязгаарлах нь бусад нэрийн маягтуудыг (жишээ нь, цахим шуудангийн хаяг) ашиглахаас хамгаалдаггүй.

X.509 нь нэрсийг хоёрдмол утгагүй байлгахыг үүрэг болгосон ч хамааралгүй хоёр эрх бүхий байгууллага ижил гаргагчийн нэрээр гэрчилгээ болон/эсвэл ХГЖ гаргах эрсдэлтэй.

Үнэт цаас гаргагчийн нэрийн зөрчилтэй холбоотой асуудал, аюулгүй байдлын асуудлуудыг багасгахын тулд ГОБ болон ХГЖ гаргагчийн нэрийг нэрийн зөрчилдөөний магадлалыг бууруулах арга замаар бүрдүүлэх ХЭРЭГТЭЙ.

Хэрэгжүүлэгчид ижил нэртэй олон хамааралгүй ГОБ болон ХГЖ гаргагч байж болзошгүйг анхаарч үзэх хэрэгтэй.

Наад зах нь ХГЖ-ийг баталгаажуулах хэрэгжүүлэлтүүд нь гэрчилгээний баталгаажуулалтын зам болон гэрчилгээг баталгаажуулахад ашигласан ХГЖ гаргагчийн баталгаажуулалтын зам нь нэг итгэлцлийн зангуугаар дуусгавар болохыг баталгаажуулах ёстой.

Цахим шуудангийн хаягийн локал хэсэг нь том жижиг үсгийн мэдрэмжтэй [RFC2821] боловч emailAddress атрибутын утгууд нь том жижиг үсгээр ялгагддаггүй [RFC2985].

Үүний үр дүнд, хэрэв и-мэйлийн сервер нь шуудангийн хайрцгийн локал хэсгүүдийн жижиг үсгийн мэдрэмжийг ашигладаг бол emailAddress шинж чанарын тохирох дүрмийг ашиглах үед хоёр өөр и-мэйл хаягийг ижил хаяг гэж үзэх эрсдэлтэй.

Хэрэв и-мэйл хаягийг эзэмшдэг и-мэйл сервер нь и-мэйл хаягийн дотоод хэсгийг жижиг үсгээр том жижиг үсгээр хардаг бол хэрэгжүүлэгчид emailAddress шинж чанарт и-мэйл хаяг оруулах ёсгүй.

Гэмтсэн гэрчилгээ эсвэл ХГЖ-ийн ХГЖ түгээх цэгүүд эсвэл эрх бүхий мэдээллийн хандалтын өргөтгөлүүд нь хортой кодын холбоосыг агуулж байвал хэрэгжүүлэгчид эрсдэлийн талаар мэдэж байх ёстой.

Хэрэгжүүлэгчид өгөгдлийг зөв бүрдүүлэхийн тулд олж авсан өгөгдлийг баталгаажуулах алхмуудыг үргэлж хийх ёстой.

Гэрчилгээнүүдэд https URI эсвэл ижил төстэй схем бүхий cRLDistributionPoints өргөтгөл орсон бол дугуй хамаарлыг нэвтрүүлж болно.

Анхны замын баталгаажуулалтыг дуусгахад шаардлагатай ХГЖ-ийг авахын тулд найдах тал нэмэлт замын баталгаажуулалт хийхээс өөр аргагүй болсон! Тойрог нөхцөлийг authorityInfoAccess эсвэл subjectInfoAccess өргөтгөл дэх https URI (эсвэл ижил төстэй схем) ашиглан үүсгэж болно.

Мууган бодоход энэ нөхцөл байдал шийдэгдээгүй хамаарал үүсгэж болзошгүй.

ГОБ-д https, ldaps эсвэл өргөтгөл дэх ижил төстэй схемүүдийг зааж өгсөн URI-г ОРУУЛАХ ЁСТОЙ.

Эдгээр өргөтгөлүүдийн аль нэгэнд https URI орсон ГОБ нь серверийн гэрчилгээг URI-д заасан мэдээллийг ашиглахгүйгээр баталгаажуулах ёстой.

cRLDistributionPoints, authorityInfoAccess эсвэл subjectInfoAccess өргөтгөлүүдээс https URI-ээр заагдсан мэдээллийг олж авахдаа серверийн

гэрчилгээг баталгаажуулахаар сонгосон итгэмжлэгдсэн талууд энэ нь хязгааргүй рекурс үүсэхэд бэлэн байх ёстой.

Өөрөө олгосон гэрчилгээ нь ГОБ-д ГОБ- ийн үйл ажиллагаанд гарсан өөрчлөлтийг харуулах нэг автомат механизмаар хангадаг.

Ялангуяа, өөрөөсөө гаргасан гэрчилгээг нэг эвдрэлгүй ГОБ түлхүүрийн хосоос нөгөөд нь хялбархан өөрчлөхөд ашиглаж болно.

" ГОБ түлхүүрийн шинэчлэлт"-ийн нарийвчилсан журмыг [RFC4210]-д заасан бөгөөд ГОБ нь өмнөх хувийн түлхүүрээ ашиглан шинэ нийтийн түлхүүрээ хамгаалдаг ба эсрэгээр нь өөрөө олгосон хоёр гэрчилгээг ашиглан хамгаалдаг.

Үйлчлүүлэгчийн хэрэгжилтийг хангаснаар өөрөө олгосон гэрчилгээг боловсруулж, шинэ түлхүүрийн дагуу олгосон гэрчилгээнд итгэж болох эсэхийг тодорхойлно.

Өөрөө олгосон гэрчилгээг ижил төстэй процедурыг ашиглан ГОБ-н бодлогын багцад нэмэлт оруулах гэх мэт ГОБ-н үйл ажиллагаанд бусад өөрчлөлтийг дэмжихэд ашиглаж болно.

Зарим хуучин хэрэгжүүлэлт нь ISO 8859-1 тэмдэгтийн багц (Latin1String) [ISO8859]-д кодлогдсон нэрийг дэмждэг боловч тэдгээрийг TeletexString гэж тэмдэглэдэг.

TeletexString нь ISO 8859-1-ээс том тэмдэгтүүдийг кодолдог боловч зарим тэмдэгтүүдийг өөрөөр кодолдог.

Хэсэг 7.1-д заасан нэрийн харьцуулалтын дүрмүүд нь TeletexStrings нь ASN.1 стандартад заасны дагуу кодлогдсон гэж үздэг.

Latin1String тэмдэгтийн багц ашиглан кодлогдсон нэрсийг харьцуулахдаа худал эерэг ба сөрөг байж болно.

Мөрүүдийг дотоод дүрслэлээс визуал дүрслэл рүү буулгах үед заримдаа хоёр өөр мөр нь ижил эсвэл ижил төстэй дүрслэлтэй байх болно.

Энэ нь олон янзын шалтгааны улмаас тохиолдож болно, тухайлбал ижил төстэй глиф ашиглах, зохиосон тэмдэгт ашиглах (жишээ нь e + ' U+00E9-тэй тэнцэх, солонгос хэлний зохиосон тэмдэгт, зарим хэл дээрх гийгүүлэгчийн бөөгнөрөл дээрх эгшиг гэх мэт).

Ийм нөхцөл байдлын үр дүнд хоёр өөр нэрийг нүдээр харьцуулж байгаа хүмүүс яг үнэндээ тийм биш гэж боддог. Мөн хүмүүс нэг мөрийг нөгөө мөр гэж андуурч магадгүй.

Гэрчилгээ гаргагчид болон итгэмжлэгдсэн талууд энэ байдлыг мэдэж байх ёстой.

9. IANA Considerations

Гэрчилгээ дэх өргөтгөлүүд болон ХГЖ-уудыг объектын адилтгагчуудаар танина.

Объектуудыг IANA-аас НТДБХ Ажлын хэсэгт хуваарилсан нуман хэлбэрээр тодорхойлсон.

Энэхүү баримт бичиг эсвэл хүлээгдэж буй шинэчлэлтүүдэд IANA-аас нэмэлт арга хэмжээ авах шаардлагагүй.

10. Acknowledgments

Warwick Ford participated with the authors in some of the design team meetings that directed development of this document. The design team's efforts were guided by contributions from Matt Crawford, Tom Gindin, Steve Hanna, Stephen Henson, Paul Hoffman, Takashi Ito, Denis Pinkas, and Wen-Cheng Wang.

11. Ном зүй

11.1 Норматив лавлагаа

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC1034] Mockapetris, P., "Domain Names- Concepts and Facilities", STD 13, RFC 1034, November 1987.

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts- - Application and Support", STD 3, RFC 1123, October 1989.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol- - HTTP/1.1", RFC 2616, June 1999.

[RFC2797] Myers, M., Liu, X., Schaad, J., and J. Weinstein, "Certificate Management

Messages over CMS", RFC 2797, April 2000.

[RFC2821] Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[RFC3454] Hoffman, P. and M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", RFC 3454, December 2002.

[RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC3987] Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)", RFC 3987, January 2005.

[RFC4516] Smith, M., Ed., and T. Howes, "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator", RFC 4516, June 2006.

[RFC4518] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation", RFC 4518, June 2006.

[RFC4523] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

[X.680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information technology- Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information technology- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

11.1 Мэдээллийн чанартай лавлагаа

[ISO8859] ISO/IEC 8859-1:1998. Information technology- - 8-bit single-byte coded graphic character sets- - Part 1: Latin alphabet No. 1.

[ISO10646] ISO/IEC 10646:2003. Information technology – Universal Multiple-Octet Coded Character Set (UCS).

[NFC] Davis, M. and M. Duerst, "Unicode Standard Annex #15: Unicode Normalization Forms", October 2006, <http://www.unicode.org/reports/tr15/>.

[RFC1422] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

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

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol- OCSP", RFC 2560, June 1999.

[RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, November 2000.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005.

[RFC4325] Santesson, S. and R. Housley, "Internet X.509 Public KeyInfrastructure Authority Information Access CertificateRevocation List (CRL) Extension", RFC 4325, December 2005.

[RFC4491] Leontiev, S., Ed., and D. Shefanovski, Ed., "Using theGOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, May 2006.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4512] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, June 2006.

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[RFC4630] Housley, R. and S. Santesson, "Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4630, August 2006.

[X.500] ITU-T Recommendation X.500 (2005) | ISO/IEC 9594-1:2005, Information technology- Open Systems Interconnection- The Directory: Overview of concepts, models and services.

[X.501] ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, Information technology- Open Systems Interconnection- The Directory: Models.

[X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology- Open Systems Interconnection- The Directory: Public-key and attribute certificate frameworks.

[X.520] ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2005, Information technology- Open Systems Interconnection- The Directory: Selected attribute types.

[X.660] ITU-T Recommendation X.660 (2004) | ISO/IEC 9834-1:2005, Information technology- Open Systems Interconnection- Procedures for the operation of OSI Registration Authorities: General procedures, and top arcs of the ASN.1 Object Identifier tree.

[X.683] ITU-T Recommendation X.683 (2002) | ISO/IEC 8824-4:2002, Information technology- Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.

[X9.55] ANSI X9.55-1997, Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists, January 1997.

ХАВСРАЛТ А – Псевдо-ASN.1-ийн бүтэц, OIDs

Энэ хавсралтаар ”ASN.1- тэй төстэй” синтакс дахь НТДБ-ийн бүрэлдэхүүнд нийцсэн өгөгдлийн объектуудыг тайлбарласан. Энэ хавсралт нь 1988 болон 1993 оны ASN.1 синтаксуудын холимог юм. 1988 оны ASN.1 синтакс нь 1993 оны UniversalString, BMPString, UTF8String төрлийн UNIVERSAL- аар өргөтгөсөн байна.

ASN.1 синтакс нь ASN.1 модульд төрлийг илэрхийлэх утга оруулахыг зөвшөөрдөггүй бөгөөд 1993 оны ASN.1 стандартад 1988 оны синтаксыг ашиглан модульд шинэ UNIVERSAL төрөл ашиглахыг зөвшөөрдөггүй. Үүний үр дүнд энэ модуль ASN.1 стандартын аль ч хувилбарт нийцэхгүй.

Энэ хавсралтыг UNIVERSAL төрлийн тодорхойлолтыг 1988 оны "ANY- ээр сольж 1988 оны ASN.1 болгон өөрчилж болно.

A.1. Тодорхой тэмдэглэгдсэн модулиуд, 1988 оны синтакс

```
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18) }

DEFINITIONS  EXPLICIT  TAGS ::=

BEGIN

-- EXPORTS ALL- -

-- IMPORTS NONE- -

-- UNIVERSAL Types defined in 1993 and 1998 ASN.1
-- and required by this specification

UniversalString ::= [UNIVERSAL 28] IMPLICIT  OCTET  STRING
      - - UniversalString is defined in ASN.1:1993

BMPString ::= [UNIVERSAL 30] IMPLICIT  OCTET  STRING
    - - BMPString is the subtype of UniversalString and models
    - - the Basic Multilingual Plane of ISO/IEC 10646

UTF8String  ::= [UNIVERSAL 12] IMPLICIT  OCTET  STRING
    - - The  content of this type conforms to RFC 3629.

-- PKIX specific OIDs
```

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

id-pe OBJECT  IDENTIFIER  ::= { id-pkix 1 }
      - - arc for private certificate extensions
id-qt OBJECT IDENTIFIER  ::= { id-pkix 2 }
      - - arc for policy qualifier types
id-kp OBJECT IDENTIFIER  ::= { id-pkix 3 }
      - - arc for extended key purpose OIDS
id-ad OBJECT  IDENTIFIER  ::= { id-pkix 48 }
      - - arc for access descriptors

-- policyQualifierIds for Internet policy qualifiers

id-qt-cps      OBJECT IDENTIFIER  ::=  { id-qt 1 }
    - - OID for CPS qualifier
id-qt-unotice  OBJECT IDENTIFIER  ::=  { id-qt 2 }
    - - OID for user notice qualifier

-- access descriptor definitions

id-ad-ocsp         OBJECT IDENTIFIER  ::= { id-ad 1 }
id-ad-calssuers    OBJECT IDENTIFIER  ::= { id-ad 2 }
id-ad-timeStamping OBJECT IDENTIFIER  ::= { id-ad 3 }
id-ad-caRepository OBJECT IDENTIFIER  ::= { id-ad 5 }

-- attribute data types

Attribute              ::= SEQUENCE  {
    type            AttributeType,
    values    SET OF  AttributeValue }
        - - at least one value is required

AttributeType          ::= OBJECT IDENTIFIER

AttributeValue         ::= ANY- - DEFINED BY AttributeType

AttributeTypeAndValue   ::= SEQUENCE  {
       type    AttributeType,
       value   AttributeValue }
```

-- санал болгож буй нэрийн шинж чанарууд: Дараах тодорхойлолт мэдээллийн объектын багцыг дотоод шаардлагад нийцүүлэн өөрчилж болно. Багцын гишүүдийг устгах нь нийцсэн

хэрэгжүүлэлттэй харилцан ажиллахад саад учруулж болзошгүйг анхаарна уу.
-- хосоор үзүүлэв: AttributeType, дараа нь харгалзах AttributeValue-ийн төрлийн тодорхойлолт.

```
id-at OBJECT IDENTIFIER  ::= { joint-iso-ccitt(2) ds(5) 4 }

-- Naming attributes of type X520name

id-at-name                AttributeType ::= { id-at 41 }
id-at-surname             AttributeType ::= { id-at  4 }
id-at-givenName           AttributeType ::= { id-at 42 }
id-at-initials            AttributeType ::= { id-at 43 }
id-at-generationQualifier AttributeType ::= { id-at 44 }

-- Naming attributes of type X520Name:
--   X520name ::= DirectoryString (SIZE (1..ub-name))
--
-- Expanded to avoid parameterized type:
X520name ::= CHOICE  {
     teletexString     TeletexString    (SIZE (1..ub-name)),
     printableString   PrintableString  (SIZE (1..ub-name)),
     universalString   UniversalString  (SIZE (1..ub-name)),
     utf8String        UTF8String       (SIZE (1..ub-name)),
     bmpString         BMPString        (SIZE (1..ub-name)) }

-- Naming attributes of type X520CommonName

id-at-commonName        AttributeType ::= { id-at 3 }

-- Naming attributes of type X520CommonName:
--   X520CommonName ::= DirectoryName (SIZE (1..ub-common-name))
--
-- Expanded to avoid parameterized type:
X520CommonName ::= CHOICE  {
     teletexString     TeletexString    (SIZE (1..ub-common-name)),
     printableString   PrintableString  (SIZE (1..ub-common-name)),
     universalString   UniversalString  (SIZE (1..ub-common-name)),
     utf8String        UTF8String       (SIZE (1..ub-common-name)),
     bmpString         BMPString        (SIZE (1..ub-common-name)) }

-- Naming attributes of type X520LocalityName

id-at-localityName      AttributeType ::= { id-at 7 }

-- Naming attributes of type X520LocalityName:
```

```
--   X520LocalityName ::= DirectoryName (SIZE (1..ub-locality-name))
--
-- Expanded to avoid parameterized type:
X520LocalityName ::= CHOICE {
     teletexString     TeletexString   (SIZE (1..ub-locality-name)),
     printableString   PrintableString (SIZE (1..ub-locality-name)),
     universalString   UniversalString (SIZE (1..ub-locality-name)),
     utf8String        UTF8String      (SIZE (1..ub-locality-name)),
     bmpString         BMPString       (SIZE (1..ub-locality-name)) }

-- Naming attributes of type X520StateOrProvinceName

id-at-stateOrProvinceName  AttributeType ::= { id-at 8 }

-- Naming attributes of type X520StateOrProvinceName:
--   X520StateOrProvinceName ::= DirectoryName (SIZE (1..ub-state-name))
--
-- Expanded to avoid parameterized type:
X520StateOrProvinceName ::= CHOICE {
     teletexString     TeletexString   (SIZE (1..ub-state-name)),
     printableString   PrintableString (SIZE (1..ub-state-name)),
     universalString   UniversalString (SIZE (1..ub-state-name)),
     utf8String        UTF8String      (SIZE (1..ub-state-name)),
     bmpString         BMPString       (SIZE (1..ub-state-name)) }

-- Naming attributes of type X520OrganizationName

id-at-organizationName   AttributeType ::= { id-at 10 }

-- Naming attributes of type X520OrganizationName:
--   X520OrganizationName ::=
--        DirectoryName (SIZE (1..ub-organization-name))
--
-- Expanded to avoid parameterized type:
X520OrganizationName ::= CHOICE {
     teletexString     TeletexString
                       (SIZE (1..ub-organization-name)),
     printableString   PrintableString
                       (SIZE (1..ub-organization-name)),
     universalString   UniversalString
                       (SIZE (1..ub-organization-name)),
     utf8String        UTF8String
                       (SIZE (1..ub-organization-name)),
     bmpString         BMPString
                       (SIZE (1..ub-organization-name))   }
```

```
-- Naming attributes of type X520OrganizationalUnitName

id-at-organizationalUnitName  AttributeType ::= { id-at 11 }

-- Naming attributes of type X520OrganizationalUnitName:
--   X520OrganizationalUnitName  ::=
--         DirectoryName (SIZE (1..ub-organizational-unit-name))
--
-- Expanded to avoid parameterized type:
X520OrganizationalUnitName  ::= CHOICE  {
     teletexString     TeletexString
                    (SIZE (1..ub-organizational-unit-name)),
     printableString   PrintableString
                    (SIZE (1..ub-organizational-unit-name)),
     universalString   UniversalString
                    (SIZE (1..ub-organizational-unit-name)),
     utf8String        UTF8String
                    (SIZE (1..ub-organizational-unit-name)),
     bmpString         BMPString
                    (SIZE (1..ub-organizational-unit-name))  }

-- Naming attributes of type X520Title

id-at-title            AttributeType ::= { id-at 12 }

-- Naming attributes of type X520Title:
--   X520Title ::= DirectoryName (SIZE (1..ub-title))
--
-- Expanded to avoid parameterized type:
X520Title ::= CHOICE  {
     teletexString     TeletexString   (SIZE (1..ub-title)),
     printableString   PrintableString (SIZE (1..ub-title)),
     universalString   UniversalString (SIZE (1..ub-title)),
     utf8String        UTF8String      (SIZE (1..ub-title)),
     bmpString         BMPString       (SIZE (1..ub-title)) }

-- Naming attributes of type X520dnQualifier

id-at-dnQualifier       AttributeType ::= { id-at 46 }

X520dnQualifier ::=     PrintableString

-- Naming attributes of type X520countryName (digraph from IS 3166)
```

```
id-at-countryName       AttributeType ::= { id-at 6 }

X520countryName ::=     PrintableString (SIZE (2))

-- Naming attributes of type X520SerialNumber

id-at-serialNumber      AttributeType ::= { id-at 5 }

X520SerialNumber ::=    PrintableString (SIZE (1..ub-serial-number))

-- Naming attributes of type X520Pseudonym

id-at-pseudonym         AttributeType ::= { id-at 65 }

-- Naming attributes of type X520Pseudonym:
--   X520Pseudonym ::= DirectoryName (SIZE (1..ub-pseudonym))
--
-- Expanded to avoid parameterized type:
X520Pseudonym ::= CHOICE  {
  teletexString     TeletexString   (SIZE (1..ub-pseudonym)),
  printableString   PrintableString (SIZE (1..ub-pseudonym)),
  universalString   UniversalString (SIZE (1..ub-pseudonym)),
  utf8String        UTF8String      (SIZE (1..ub-pseudonym)),
  bmpString         BMPString       (SIZE (1..ub-pseudonym)) }

-- Naming attributes of type DomainComponent (from RFC 4519)

id-domainComponent   AttributeType ::= { 0 9 2342 19200300 100 1 25 }

DomainComponent ::=  IA5String

-- Legacy attributes

pkcs-9 OBJECT IDENTIFIER  ::=
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }

id-emailAddress      AttributeType ::= { pkcs-9 1 }

EmailAddress ::=     IA5String (SIZE (1..ub-emailaddress-length))

-- naming data types--

Name ::= CHOICE  {-- only one possibility for now--
     rdnSequence   RDNSequence }
```

```
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

DistinguishedName ::=  RDNSequence

RelativeDistinguishedName ::= SET SIZE (1..MAX) OF AttributeTypeAndValue

-- Directory string type--

DirectoryString ::= CHOICE {
      teletexString       TeletexString   (SIZE (1..MAX)),
      printableString     PrintableString (SIZE (1..MAX)),
      universalString     UniversalString (SIZE (1..MAX)),
      utf8String          UTF8String      (SIZE (1..MAX)),
      bmpString           BMPString       (SIZE (1..MAX)) }

-- certificate and CRL specific structures begin here

Certificate ::= SEQUENCE  {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signature           BIT STRING   }

TBSCertificate ::= SEQUENCE  {
    version        [0]  Version DEFAULT v1,
    serialNumber         CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                         -- If present, version MUST be v2 or v3
    subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                         -- If present, version MUST be v2 or v3
    extensions      [3]  Extensions OPTIONAL
                         -- If present, version MUST be v3--  }

Version ::= INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time  }
```

```
Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
    algorithm           AlgorithmIdentifier,
    subjectPublicKey    BIT STRING   }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING
                - - contains the DER encoding of an ASN.1 value
                - - corresponding to the extension type identified
                - - by extnID
    }

-- CRL structures

CertificateList  ::=  SEQUENCE  {
    tbsCertList          TBSCertList,
    signatureAlgorithm   AlgorithmIdentifier,
    signature            BIT STRING   }

TBSCertList  ::=  SEQUENCE  {
    version                 Version OPTIONAL,
                            - - if present, MUST be v2
    signature               AlgorithmIdentifier,
    issuer                  Name,
    thisUpdate               Time,
    nextUpdate               Time OPTIONAL,
    revokedCertificates     SEQUENCE OF SEQUENCE  {
        userCertificate         CertificateSerialNumber,
        revocationDate           Time,
        crlEntryExtensions      Extensions OPTIONAL
                                - - if present, version MUST be v2
                            }  OPTIONAL,
    crlExtensions           [0] Extensions OPTIONAL }
                            - - if present, version MUST be v2

-- Version, Time, CertificateSerialNumber, and Extensions were
```

```
-- defined earlier for use in the certificate structure

AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL }
                            -- contains a value of the type
                            -- registered for use with the
                            -- algorithm object identifier value

-- X.400 address syntax starts here

ORAddress ::= SEQUENCE {
  built-in-standard-attributes BuiltInStandardAttributes,
  built-in-domain-defined-attributes
                BuiltInDomainDefinedAttributes OPTIONAL,
 -- see also teletex-domain-defined-attributes
  extension-attributes ExtensionAttributes OPTIONAL }

-- Built-in Standard Attributes

BuiltInStandardAttributes ::= SEQUENCE {
  country-name                  CountryName OPTIONAL,
  administration-domain-name    AdministrationDomainName OPTIONAL,
  network-address           [0] IMPLICIT NetworkAddress OPTIONAL,
   -- see also extended-network-address
  terminal-identifier       [1] IMPLICIT TerminalIdentifier OPTIONAL,
  private-domain-name       [2] PrivateDomainName OPTIONAL,
  organization-name         [3] IMPLICIT OrganizationName OPTIONAL,
   -- see also teletex-organization-name
  numeric-user-identifier   [4] IMPLICIT NumericUserIdentifier
                            OPTIONAL,
  personal-name             [5] IMPLICIT PersonalName OPTIONAL,
   -- see also teletex-personal-name
  organizational-unit-names [6] IMPLICIT OrganizationalUnitNames
                            OPTIONAL }
   -- see also teletex-organizational-unit-names

CountryName ::= [APPLICATION 1] CHOICE {
  x121-dcc-code         NumericString
                        (SIZE (ub-country-name-numeric-length)),
  iso-3166-alpha2-code  PrintableString
                        (SIZE (ub-country-name-alpha-length)) }

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
  numeric   NumericString   (SIZE (0..ub-domain-name-length)),
```

```
   printable PrintableString (SIZE (0..ub-domain-name-length)) }

NetworkAddress ::= X121Address - - see also extended-network-address

X121Address ::= NumericString (SIZE (1..ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE (1..ub-terminal-id-length))

PrivateDomainName ::= CHOICE {
   numeric   NumericString   (SIZE (1..ub-domain-name-length)),
   printable PrintableString (SIZE (1..ub-domain-name-length)) }

OrganizationName ::= PrintableString
                     (SIZE (1..ub-organization-name-length))
 - - see also teletex-organization-name

NumericUserIdentifier ::= NumericString
                     (SIZE (1..ub-numeric-user-id-length))

PersonalName ::= SET {
   surname      [0] IMPLICIT PrintableString
                (SIZE (1..ub-surname-length)),
   given-name   [1] IMPLICIT PrintableString
                (SIZE (1..ub-given-name-length)) OPTIONAL,
   initials     [2] IMPLICIT PrintableString
                (SIZE (1..ub-initials-length)) OPTIONAL,
   generation-qualifier [3] IMPLICIT PrintableString
                (SIZE (1..ub-generation-qualifier-length))
                OPTIONAL }
 - - see also teletex-personal-name

OrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units)
                     OF OrganizationalUnitName
 - - see also teletex-organizational-unit-names

OrganizationalUnitName ::= PrintableString (SIZE
                (1..ub-organizational-unit-name-length))

-- Built-in Domain-defined Attributes

BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE
                (1..ub-domain-defined-attributes) OF
                BuiltInDomainDefinedAttribute

BuiltInDomainDefinedAttribute ::= SEQUENCE {
```

```
  type PrintableString (SIZE
            (1..ub-domain-defined-attribute-type-length)),
  value PrintableString (SIZE
            (1..ub-domain-defined-attribute-value-length)) }

-- Extension Attributes

ExtensionAttributes ::= SET SIZE (1..ub-extension-attributes) OF
            ExtensionAttribute

ExtensionAttribute ::=  SEQUENCE {
  extension-attribute-type [0] IMPLICIT  INTEGER
            (0..ub-extension-attributes),
  extension-attribute-value  [1]
            ANY DEFINED BY extension-attribute-type }

-- Extension types and attribute values

common-name INTEGER  ::= 1

CommonName ::= PrintableString (SIZE (1..ub-common-name-length))

teletex-common-name INTEGER  ::= 2

TeletexCommonName  ::= TeletexString (SIZE (1..ub-common-name-length))

teletex-organization-name  INTEGER  ::= 3

TeletexOrganizationName  ::=
            TeletexString  (SIZE (1..ub-organization-name-length))

teletex-personal-name  INTEGER  ::= 4

TeletexPersonalName  ::= SET {
  surname      [0] IMPLICIT  TeletexString
               (SIZE (1..ub-surname-length)),
  given-name  [1] IMPLICIT  TeletexString
               (SIZE (1..ub-given-name-length))  OPTIONAL,
  initials    [2] IMPLICIT  TeletexString
               (SIZE (1..ub-initials-length)) OPTIONAL,
  generation-qualifier [3] IMPLICIT  TeletexString
               (SIZE (1..ub-generation-qualifier-length))
               OPTIONAL  }

teletex-organizational-unit-names  INTEGER  ::= 5
```

```
TeletexOrganizationalUnitNames  ::= SEQUENCE  SIZE
     (1..ub-organizational-units)  OF TeletexOrganizationalUnitName

TeletexOrganizationalUnitName  ::= TeletexString
               (SIZE (1..ub-organizational-unit-name-length))

pds-name INTEGER  ::= 7

PDSName ::= PrintableString (SIZE (1..ub-pds-name-length))

physical-delivery-country-name INTEGER  ::= 8

PhysicalDeliveryCountryName  ::= CHOICE  {
   x121-dcc-code NumericString  (SIZE (ub-country-name-numeric-length)),
   iso-3166-alpha2-code  PrintableString
                        (SIZE (ub-country-name-alpha-length))  }

postal-code INTEGER  ::= 9

PostalCode ::= CHOICE  {
   numeric-code    NumericString  (SIZE (1..ub-postal-code-length)),
   printable-code PrintableString  (SIZE (1..ub-postal-code-length)) }

physical-delivery-office-name INTEGER  ::= 10

PhysicalDeliveryOfficeName ::= PDSParameter

physical-delivery-office-number INTEGER  ::= 11

PhysicalDeliveryOfficeNumber ::= PDSParameter

extension-OR-address-components INTEGER  ::= 12

ExtensionORAddressComponents ::= PDSParameter

physical-delivery-personal-name  INTEGER  ::= 13

PhysicalDeliveryPersonalName  ::= PDSParameter

physical-delivery-organization-name  INTEGER  ::= 14

PhysicalDeliveryOrganizationName  ::= PDSParameter

extension-physical-delivery-address-components INTEGER  ::= 15
```

```
ExtensionPhysicalDeliveryAddressComponents ::= PDSParameter

unformatted-postal-address INTEGER  ::= 16

UnformattedPostalAddress ::= SET{
  printable-address SEQUENCE SIZE (1..ub-pds-physical-address-lines)
      OF PrintableString (SIZE (1..ub-pds-parameter-length))  OPTIONAL,
  teletex-string TeletexString
      (SIZE (1..ub-unformatted-address-length)) OPTIONAL  }

street-address INTEGER  ::= 17

StreetAddress ::= PDSParameter

post-office-box-address INTEGER ::= 18

PostOfficeBoxAddress ::= PDSParameter

poste-restante-address INTEGER  ::= 19

PosteRestanteAddress ::= PDSParameter

unique-postal-name  INTEGER  ::= 20

UniquePostalName  ::= PDSParameter

local-postal-attributes INTEGER  ::= 21

LocalPostalAttributes ::= PDSParameter

PDSParameter ::= SET {
  printable-string PrintableString
          (SIZE(1..ub-pds-parameter-length))  OPTIONAL,
  teletex-string TeletexString
          (SIZE(1..ub-pds-parameter-length))  OPTIONAL  }

extended-network-address INTEGER  ::= 22

ExtendedNetworkAddress ::= CHOICE  {
  e163-4-address  SEQUENCE  {
    number      [0] IMPLICIT  NumericString
                (SIZE  (1..ub-e163-4-number-length)),
    sub-address [1] IMPLICIT  NumericString
                (SIZE  (1..ub-e163-4-sub-address-length))
```

```
                    OPTIONAL },
  psap-address  [0] IMPLICIT  PresentationAddress }

PresentationAddress ::= SEQUENCE {
    pSelector     [0] EXPLICIT  OCTET  STRING  OPTIONAL,
    sSelector     [1] EXPLICIT  OCTET  STRING  OPTIONAL,
    tSelector     [2] EXPLICIT  OCTET  STRING  OPTIONAL,
    nAddresses    [3] EXPLICIT  SET SIZE  (1..MAX) OF OCTET  STRING  }

terminal-type  INTEGER  ::= 23

TerminalType  ::= INTEGER  {
  telex        (3),
  teletex      (4),
  g3-facsimile (5),
  g4-facsimile (6),
  ia5-terminal  (7),
  videotex     (8) } (0..ub-integer-options)

-- Extension Domain-defined Attributes

teletex-domain-defined-attributes INTEGER  ::= 6

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE
  (1..ub-domain-defined-attributes) OF TeletexDomainDefinedAttribute

TeletexDomainDefinedAttribute ::= SEQUENCE  {
       type TeletexString
            (SIZE (1..ub-domain-defined-attribute-type-length)),
       value TeletexString
            (SIZE (1..ub-domain-defined-attribute-value-length))  }

--  specifications of Upper Bounds MUST be regarded as mandatory
--  from Annex B of ITU-T X.411 Reference Definition of MTS Parameter
--  Upper Bounds

-- Upper Bounds
ub-name INTEGER  ::= 32768
ub-common-name INTEGER  ::= 64
ub-locality-name INTEGER  ::= 128
ub-state-name  INTEGER  ::= 128
ub-organization-name  INTEGER  ::= 64
ub-organizational-unit-name  INTEGER  ::= 64
ub-title INTEGER  ::= 64
ub-serial-number  INTEGER  ::= 64
```

```
ub-match INTEGER ::= 128
ub-emailaddress-length INTEGER ::= 255
ub-common-name-length INTEGER ::= 64
ub-country-name-alpha-length INTEGER ::= 2
ub-country-name-numeric-length INTEGER ::= 3
ub-domain-defined-attributes INTEGER ::= 4
ub-domain-defined-attribute-type-length INTEGER ::= 8
ub-domain-defined-attribute-value-length INTEGER ::= 128
ub-domain-name-length INTEGER ::= 16
ub-extension-attributes INTEGER ::= 256
ub-e163-4-number-length INTEGER ::= 15
ub-e163-4-sub-address-length INTEGER ::= 40
ub-generation-qualifier-length INTEGER ::= 3
ub-given-name-length INTEGER ::= 16
ub-initials-length INTEGER ::= 5
ub-integer-options INTEGER ::= 256
ub-numeric-user-id-length INTEGER ::= 32
ub-organization-name-length INTEGER ::= 64
ub-organizational-unit-name-length INTEGER ::= 32
ub-organizational-units INTEGER ::= 4
ub-pds-name-length INTEGER ::= 16
ub-pds-parameter-length INTEGER ::= 30
ub-pds-physical-address-lines INTEGER ::= 6
ub-postal-code-length INTEGER ::= 16
ub-pseudonym INTEGER ::= 128
ub-surname-length INTEGER ::= 40
ub-terminal-id-length INTEGER ::= 24
ub-unformatted-address-length INTEGER ::= 180
ub-x121-address-length INTEGER ::= 16
```

-- Тэмдэглэл- TeletexString гэх мэт мөрийн төрлүүдийн дээд хязгаарыг тэмдэгтээр хэмждэг. PrintableString эсвэл IA5String-аас бусад тохиолдолд ийм утгыг барихад илүү олон тооны октет шаардлагатай болно. Хамгийн багадаа 16 октет буюу заасан хэмжээнээс хоёр дахин их байх ёстой.

-- TeletexString. UTF8String эсвэл UniversalString-ийн хувьд дээд хязгаараас дор хаяж дөрөв дахин их байх ёстой.

A.2. Implicitly Tagged Module, 1988 Syntax

```
PKIX1Implicit88 { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-implicit(19) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
-- EXPORTS ALL- -

IMPORTS
     id-pe, id-kp, id-qt-unotice, id-qt-cps,
    - - delete following line if "new" types are supported- -
     BMPString, UTF8String,  - - end "new" types- -
     ORAddress, Name, RelativeDistinguishedName,
     CertificateSerialNumber,  Attribute, DirectoryString
     FROM PKIX1Explicit88 { iso(1) identified-organization(3)
          dod(6) internet(1) security(5) mechanisms(5) pkix(7)
          id-mod(0) id-pkix1-explicit(18) };

-- ISO arc for standard certificate and CRL extensions

id-ce OBJECT IDENTIFIER  ::=  {joint-iso-ccitt(2) ds(5) 29}

-- authority key identifier OID and syntax

id-ce-authorityKeyIdentifier OBJECT IDENTIFIER  ::=  { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE  {
    keyIdentifier             [0] KeyIdentifier           OPTIONAL,
    authorityCertIssuer       [1] GeneralNames            OPTIONAL,
    authorityCertSerialNumber  [2] CertificateSerialNumber   OPTIONAL  }
   - - authorityCertIssuer  and authorityCertSerialNumber  MUST both
   - - be present or both be absent

KeyIdentifier ::= OCTET  STRING

-- subject key identifier OID  and syntax

id-ce-subjectKeyIdentifier OBJECT  IDENTIFIER  ::=  { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier

-- key usage extension OID and syntax

id-ce-keyUsage OBJECT  IDENTIFIER  ::=  { id-ce 15 }

KeyUsage ::= BIT  STRING  {
     digitalSignature        (0),
     nonRepudiation          (1), - - recent editions of X.509 have
                          - - renamed  this bit to contentCommitment
     keyEncipherment         (2),
```

```
    dataEncipherment        (3),
    keyAgreement            (4),
    keyCertSign             (5),
    cRLSign                 (6),
    encipherOnly            (7),
    decipherOnly            (8) }

-- private key usage period extension OID and syntax

id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER  ::=  { id-ce 16 }

PrivateKeyUsagePeriod ::= SEQUENCE {
    notBefore       [0]     GeneralizedTime  OPTIONAL,
    notAfter        [1]     GeneralizedTime  OPTIONAL }
   - - either notBefore or notAfter MUST be present

-- certificate policies extension OID and syntax

id-ce-certificatePolicies OBJECT IDENTIFIER  ::=  { id-ce 32 }

anyPolicy OBJECT IDENTIFIER  ::= { id-ce-certificatePolicies 0 }

CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier   CertPolicyId,
    policyQualifiers   SEQUENCE SIZE (1..MAX) OF
            PolicyQualifierInfo OPTIONAL  }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId  PolicyQualifierId,
    qualifier          ANY DEFINED BY policyQualifierId }

-- Бодлогын нэмэлт шалгуур үзүүлэлтийг хүлээн зөвшөөрсөн хэрэгжүүлэлтүүд ЗААВАЛ
PolicyQualifierId-ийн дараах тодорхойлолтыг өөрчилнө.

PolicyQualifierId ::= OBJECT IDENTIFIER  ( id-qt-cps | id-qt-unotice )

-- CPS pointer qualifier

CPSuri ::= IA5String

-- user notice qualifier
```

```
UserNotice ::= SEQUENCE {
    noticeRef        NoticeReference OPTIONAL,
    explicitText     DisplayText OPTIONAL }

NoticeReference ::= SEQUENCE {
    organization     DisplayText,
    noticeNumbers    SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
    ia5String        IA5String      (SIZE (1..200)),
    visibleString    VisibleString  (SIZE (1..200)),
    bmpString        BMPString      (SIZE (1..200)),
    utf8String       UTF8String     (SIZE (1..200)) }

-- policy mapping extension OID and syntax

id-ce-policyMappings OBJECT IDENTIFIER  ::=  { id-ce 33 }

PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy      CertPolicyId,
    subjectDomainPolicy     CertPolicyId }

-- subject alternative name extension OID and syntax

id-ce-subjectAltName OBJECT IDENTIFIER  ::=  { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames  ::= SEQUENCE  SIZE (1..MAX) OF GeneralName

GeneralName  ::= CHOICE {
    otherName                 [0]  AnotherName,
    rfc822Name                [1]  IA5String,
    dNSName                   [2]  IA5String,
    x400Address               [3]  ORAddress,
    directoryName             [4]  Name,
    ediPartyName              [5]  EDIPartyName,
    uniformResourceIdentifier [6]  IA5String,
    iPAddress                 [7]  OCTET STRING,
    registeredID              [8]  OBJECT IDENTIFIER }

-- AnotherName replaces OTHER-NAME  ::= TYPE-IDENTIFIER,  as
-- TYPE-IDENTIFIER  is not supported in the '88 ASN.1 syntax
```

```
AnotherName ::= SEQUENCE {
    type-id    OBJECT IDENTIFIER,
    value      [0] EXPLICIT ANY DEFINED BY type-id }

EDIPartyName ::= SEQUENCE {
    nameAssigner            [0]  DirectoryString OPTIONAL,
    partyName               [1]  DirectoryString }

-- issuer alternative name extension OID and syntax

id-ce-issuerAltName OBJECT IDENTIFIER ::= { id-ce 18 }

IssuerAltName ::= GeneralNames

id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= { id-ce 9 }

SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute

-- basic constraints extension OID and syntax

id-ce-basicConstraints OBJECT IDENTIFIER ::= { id-ce 19 }

BasicConstraints ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }

-- name constraints extension OID and syntax

id-ce-nameConstraints OBJECT IDENTIFIER ::= { id-ce 30 }

NameConstraints ::= SEQUENCE {
    permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
    base                    GeneralName,
    minimum         [0]     BaseDistance DEFAULT 0,
    maximum         [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)

-- policy constraints extension OID and syntax
```

```
id-ce-policyConstraints OBJECT IDENTIFIER  ::=  { id-ce 36 }

PolicyConstraints ::= SEQUENCE {
    requireExplicitPolicy   [0]    SkipCerts OPTIONAL,
    inhibitPolicyMapping    [1]    SkipCerts OPTIONAL  }

SkipCerts ::= INTEGER  (0..MAX)

-- CRL distribution points extension OID and syntax

id-ce-cRLDistributionPoints     OBJECT IDENTIFIER   ::=  {id-ce 31}

CRLDistributionPoints ::= SEQUENCE  SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
    distributionPoint       [0]     DistributionPointName OPTIONAL,
    reasons                 [1]     ReasonFlags OPTIONAL,
    cRLIssuer               [2]     GeneralNames  OPTIONAL  }

DistributionPointName ::= CHOICE  {
    fullName                [0]     GeneralNames,
    nameRelativeToCRLIssuer  [1]    RelativeDistinguishedName }

ReasonFlags ::= BIT  STRING  {
    unused                  (0),
    keyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6),
    privilegeWithdrawn      (7),
    aACompromise            (8) }

-- extended key usage extension OID and syntax

id-ce-extKeyUsage OBJECT  IDENTIFIER  ::= {id-ce 37}

ExtKeyUsageSyntax ::= SEQUENCE  SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER

-- permit unspecified key uses

anyExtendedKeyUsage OBJECT IDENTIFIER  ::= { id-ce-extKeyUsage 0 }
```

```
-- extended key purpose OIDs

id-kp-serverAuth            OBJECT IDENTIFIER  ::= { id-kp 1 }
id-kp-clientAuth            OBJECT IDENTIFIER  ::= { id-kp 2 }
id-kp-codeSigning           OBJECT IDENTIFIER  ::= { id-kp 3 }
id-kp-emailProtection       OBJECT IDENTIFIER  ::= { id-kp 4 }
id-kp-timeStamping          OBJECT IDENTIFIER  ::= { id-kp 8 }
id-kp-OCSPSigning           OBJECT IDENTIFIER  ::= { id-kp 9 }

-- inhibit any policy OID and syntax

id-ce-inhibitAnyPolicy OBJECT IDENTIFIER  ::=  { id-ce 54 }

InhibitAnyPolicy ::= SkipCerts

-- freshest (delta)CRL  extension OID and syntax

id-ce-freshestCRL OBJECT IDENTIFIER  ::=  { id-ce 46 }

FreshestCRL  ::= CRLDistributionPoints

-- authority info access

id-pe-authorityInfoAccess OBJECT IDENTIFIER  ::= { id-pe 1 }

AuthorityInfoAccessSyntax  ::=
      SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription  ::=  SEQUENCE {
      accessMethod          OBJECT IDENTIFIER,
      accessLocation        GeneralName   }

-- subject info access

id-pe-subjectInfoAccess OBJECT IDENTIFIER  ::= { id-pe 11 }

SubjectInfoAccessSyntax  ::=
      SEQUENCE SIZE (1..MAX) OF AccessDescription

-- CRL number extension OID and syntax

id-ce-cRLNumber OBJECT IDENTIFIER  ::= { id-ce 20 }

CRLNumber  ::= INTEGER  (0..MAX)
```

```
-- issuing distribution point extension OID and syntax

id-ce-issuingDistributionPoint OBJECT IDENTIFIER  ::= { id-ce 28 }

IssuingDistributionPoint ::= SEQUENCE {
     distributionPoint          [0] DistributionPointName OPTIONAL,
     onlyContainsUserCerts      [1] BOOLEAN DEFAULT FALSE,
     onlyContainsCACerts        [2] BOOLEAN DEFAULT FALSE,
     onlySomeReasons            [3] ReasonFlags OPTIONAL,
     indirectCRL                [4] BOOLEAN DEFAULT FALSE,
     onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE }
    - - at most one of onlyContainsUserCerts, onlyContainsCACerts,
    - - and onlyContainsAttributeCerts may be set to TRUE.

id-ce-deltaCRLIndicator OBJECT IDENTIFIER  ::= { id-ce 27 }

BaseCRLNumber  ::= CRLNumber

-- reason code extension OID and syntax

id-ce-cRLReasons OBJECT IDENTIFIER  ::= { id-ce 21 }

CRLReason ::= ENUMERATED {
     unspecified             (0),
     keyCompromise           (1),
     cACompromise            (2),
     affiliationChanged      (3),
     superseded              (4),
     cessationOfOperation    (5),
     certificateHold         (6),
     removeFromCRL           (8),
     privilegeWithdrawn      (9),
     aACompromise            (10) }

-- certificate issuer CRL entry extension OID and syntax

id-ce-certificateIssuer OBJECT IDENTIFIER  ::= { id-ce 29 }

CertificateIssuer ::= GeneralNames

-- hold instruction extension OID and syntax

id-ce-holdInstructionCode OBJECT IDENTIFIER  ::= { id-ce 23 }
```

```
HoldInstructionCode ::= OBJECT IDENTIFIER

-- ANSI x9 arc holdinstruction arc

holdInstruction OBJECT IDENTIFIER  ::=
        {joint-iso-itu-t(2) member-body(2) us(840) x9cm(10040)  2}

-- ANSI X9 holdinstructions

id-holdinstruction-none OBJECT IDENTIFIER   ::=
                              {holdInstruction 1}- - deprecated

id-holdinstruction-callissuer OBJECT IDENTIFIER  ::= {holdInstruction 2}

id-holdinstruction-reject OBJECT IDENTIFIER  ::= {holdInstruction 3}

-- invalidity date CRL  entry extension OID and syntax

id-ce-invalidityDate OBJECT  IDENTIFIER  ::= { id-ce 24 }

InvalidityDate ::=  GeneralizedTime

END
```

ХАВСРАЛТ B – ASN.1 тэмдэглэл

ГОБ-ууд serialNumber- ийг ЗААВАЛ сөрөг биш бүхэл тоо байна, өөрөөр хэлбэл, INTEGER утгын DER шифрлэлт дэх sign бит ЗААВАЛ тэг байна. Шаардлагатай бол хамгийн эхэнд (хамгийн зүүн) '00'H октетыг нэмж үүнийг хийж болно. Октетын утга болон бүхэл тоон утгын хоорондох зураглалд гарч болзошгүй хоёрдмол байдлыг арилгана.

4.1.2.2- д тэмдэглэснээр сериал дугаарууд урт бүхэл тоо агуулж болно. Гэрчилгээ хэрэглэгчид уртдаа 20 октет хүртэлх урттай serialNumber- ийн утгыг ЗААВАЛ боловсруулах боломжтой байна. Хамаарах ГОБ-ууд 20 октетоос урт serialNumber утгыг ашиглаж БОЛОХГҮЙ.

5.2.3- д тэмдэглэснээр ХГЖ-ийн дугаар нь урт бүхэл тоо агуулж болно. ХГЖ баталгаажуулагч уртдаа 20 октет хүртэлх урттай cRLNumber- ийн утгыг ЗААВАЛ боловсруулах боломжтой байна. Хамаарах ГОБ-ын гэрчилгээ олгогчид 20 октетоос урт cRLNumber утгыг ашиглаж БОЛОХГҮЙ.

"SEQUENCE SIZE (1..MAX) OF" бүтэц нь хэд хэдэн ASN.1 бүтцэд харагдана. Хүчинтэй ASN.1 дараалал нь тэг эсвэл түүнээс олон бүртгэл (entry) байна. SIZE (1..MAX) бүтэц нь багадаа нэг бүртгэлтэй байх дарааллыг хязгаарладаг. MAX нь дээд хязгаар тодорхойгүй гэдгийг илэрхийлнэ. Хэрэгжүүлэлтээсээ хамааранд нь орчиндоо тохирсон дээд хязгаарыг чөлөөтэй сонгох боломжтой.

Код

Хэрэгжүүлэгчид at тэмдэг ('@'), доогуур зураас ('_') тэмдэгтүүдийг ASN.1 төрлийн PrintableString дэмждэггүй болохыг анхаарах хэрэгтэй. Эдгээр тэмдэгтүүд ихэвчлэн Интернэт хаягуудад ашиглагддаг. Ийм хаягууд нь тэдгээрийг дэмждэг ASN.1 төрлийг ашиглан кодлогдсон байх ёстой. Тэдгээр нь ихэвчлэн ялгах нэрийн доторх emailAddress шинж эсвэл GeneralName-н rfc822Name талбарт IA5String хэлбэрээр кодлогдсон байдаг. Тохиромжтой хэрэгжүүлэлтүүд нь at тэмдэг эсвэл доогуур зураасыг агуулсан мөрүүдийг ЗААВАЛ PrintableString-ээр кодолно.

Нэрлэсэн битийн жагсаалт нь нэрд оноосон утгын BIT STRINGS байна. Энэхүү тодорхойлолт нь түлхүүрийн хэрэглээ, ХГЖ- ийн түгээлтийн цэг, сүүлийн ХГЖ гэрчилгээний өргөтгөлүүдийн тодорхойлолтод нэрлэгдсэн битийн жагсаалтыг, мөн сүүлийн ХГЖ болон түгээлтийн цэгийн ХГЖ өргөтгөлүүдийг ашигладаг. DER

кодчиллоор нэрлэсэн битийн жагсаалтыг кодлох үед арын тэгүүдийг ЗААВАЛ орхино. Өөрөөр хэлбэл, кодлогдсон утга нь нэгээр тохируулагдсан сүүлчийн нэрлэсэн битээр төгсдөг.

Тэмдэгтийн мөрийн төрөл UniversalString нь [ISO10646]- аар зөвшөөрөгдсөн тэмдэгтүүдийн аль нэгийг дэмждэг. ISO 10646 нь Универсал олон октетоор кодлогдсон тэмдэгтийн багц (UCS) юм.

UTF8String тэмдэгтийн мөрийн төрлийг 1997 онд ASN.1-ийн хувилбарт танилцуулсан бөгөөд UTF8String нь [X.520]-ийн 2001 оны хувилбарт DirectoryString-ийн сонголтуудын жагсаалтад нэмэгдсэн байна. UTF8String нь универсал төрөл бөгөөд 12 гэсэн таг утга авна. UTF8String-ийн агуулгыг RFC 2044-д тодорхойлсон бөгөөд RFC 2279-д шинэчлэгдсэн энэ нь [RFC3629]-д шинэчлэгдсэн.

Эдгээр өөрчлөлтөөс [RFC2277]-д кодлогдсон IETF-ийн шилдэг туршлагууд, Тэмдэгтийн багц ба хэлний IETF-ийн бодлогод нийцүүлэн энэ баримт бичигт UTF8String-ийг DirectoryString болон userNotice гэрчилгээний бодлогын шалгуур үзүүлэлтийн сонголт болгон оруулсан болно.

[X.520]-д тодорхойлсон олон шинж чанарын хувьд AttributeValue нь DirectoryString төрлийг ашигладаг. Хавсралт А-д заасан атрибутуудаас нэр, овог, өөрийн нэр, үеийн нэр, нийтлэг нэр, байршлын нэр, муж эсвэл аймгийн нэр, байгууллагын нэр, байгууллагын Нэгжийн Нэр, гарчиг, нууц нэрийн шинж чанарууд бүгд DirectoryString төрлийг ашигладаг. X.520 нь эдгээр шинж чанаруудын синтаксийг зааж өгөхийн тулд DirectoryString-ийн параметржүүлсэн төрлийн [X.683] тодорхойлолтыг ашигладаг. Параметр нь шинж чанар бүрийн зөвшөөрөгдсөн тэмдэгтийн уртыг зааж өгөхөд ашиглагддаг. Хавсралт А-д параметржүүлсэн төрлийн тодорхойлолтыг ашиглахаас зайлсхийхийн тулд DirectoryString төрлийг эдгээр шинж чанарын төрөл бүрийн тодорхойлолтод зориулж өргөтгөсөн хэлбэрээр бичсэн болно. Тиймээс, Хавсралт А дахь ASN.1 нь эдгээр шинж чанаруудын синтаксийг TeletexString, PrintableString, UniversalString, UTF8String, BMPString гэж СОНГОЖ болохоор тодорхойлсон бөгөөд Синтаксийг тайлбарлахдаа ASN.1 төрлийн DirectoryString ашиглахын оронд СОНГОЛТ доторх төрөл тус бүрд мөрийн уртын зохих хязгаарлалтуудыг ашиглана.

SET OF утгуудын DER кодчилол нь утгуудын кодчиллын дарааллыг шаарддаг гэдгийг хэрэгжүүлэгчид анхаарах хэрэгтэй. Ялангуяа энэ асуудал ялгах нэртэй холбоотой гарч ирдэг.

АНХНЫ УТГА бүхий утгатай DER кодчиллоор кодолсон SET эсвэл SEQUENCE

бүрэлдэхүүн хэсгүүдийг гэрчилгээ эсвэл ХГЖ-аас орхидог гэдгийг хэрэгжүүлэгчид анхаарах хэрэгтэй.

Жишээ нь, cA утга нь ХУДАЛ бол BasicConstraints өргөтгөл нь кодлогдсон гэрчилгээнээс cA бүүлийн утгаас хасах болно.

Объектын адилтгагч (OIDs) нь гэрчилгээний бодлого, нийтийн түлхүүр болон гарын үсгийн алгоритм, гэрчилгээний өргөтгөл гэх мэтийг тодорхойлоход энэхүү техникийн тодорхойлолтыг ашиглагддаг. Объектын адилтгагчдад (OIDs) дээд хэмжээ байхгүй. Энэ тодорхойлолт нь 2^28-аас бага утгатай нуман элементтэй OID-д дэмжлэг үзүүлэх үүрэгтэй, өөрөөр хэлбэл тэдгээр нь ЗААВАЛ 0-оос 268,435,455-ын хооронд байх ёстой. Энэ нь нумын элемент бүрийг дан 32 бит үгээр илэрхийлэх боломжийг олгодог. Хэрэгжүүлэлтүүд нь цэгээр тусгаарласан аравтын утга бүхий ([RFC4512]-ын 1.4-р хэсгийг үзнэ үү) 100 байт (агуулсан) хүртэл байж болох OID-г ЗААВАЛ дэмжинэ. Хэрэгжүүлэлтүүд нь 20 хүртэлх элемент (агуулсан)- тэй OID-ийг зохицуулах чадвартай байх ёстой. ГОБ нь эдгээр шаардлагаас хэтэрсэн OID агуулсан гэрчилгээ олгох ёсгүй. Үүний нэгэн адил, ХГЖ олгогчид эдгээр шаардлагаас хэтэрсэн OID агуулсан ХГЖ-ыг гаргаж БОЛОХГҮЙ.

NameConstraints өргөтгөл дэх GeneralName талбарын утгыг кодлох агуулгын тусгай дүрмүүд нь бусад өргөтгөлүүдэд ашиглах дүрмээс ялгаатай. Энэ баримт бичигт заасан бусад бүх гэрчилгээ, ХГЖ болон ХГЖ-ын бичлэгийн өргөтгөлүүдэд кодчиллын дүрмүүд нь үндсэн дүрэмд нийцдэг. Жишээлбэл, uniformResourceIdentifier талбар дахь утгууд нь [RFC3986]-д заасан хүчинтэй URI-г агуулсан байх ёстой. NameConstraints өргөтгөл дэх утгыг кодлох агуулгын тусгай дүрмийг 4.2.1.10-д заасан болно, мөн эдгээр дүрмүүд нь үндсэн дүрэмд нийцэхгүй байж болно. Жишээ нь, uniformResourceIdentifier талбар нь nameConstraints өргөтгөлд гарч ирэх үед URI гэхээсээ илүү DNS нэр (жишээ нь, "host.example.com" эсвэл ".example.com") байх ёстой.

X.500 стандартын нийгэмлэг өргөтгөлийн хэд хэдэн дүрмийг боловсруулсан гэдгийг хэрэгжүүлэгчид анхааруулж байна. Эдгээр дүрмүүд нь ASN.1-ийн тодорхойлолтыг шинэ объектын адилтгагч (OID) оноохгүйгээр хэзээ өөрчлөх боломжтойг тодорхойлдог. Жишээлбэл, энэ профайлын баримт бичгийн өмнөх хувилбар болох [RFC2459]-д багтсан дор хаяж хоёр өргөтгөлийн тодорхойлолт нь энэ тодорхойлолтод өөр ASN.1 тодорхойлолттой боловч ижил OID ашигладаг. Хэрэв өргөтгөл дотор үл мэдэгдэх элементүүд гарч, өргөтгөл нь чухал гэж тэмдэглэгдээгүй бол үл мэдэгдэх элементүүдийг дараах байдлаар үл тоох хэрэгтэй.

1. битийн мөр доторх үл мэдэгдэх битийн нэрийн бүх хуваарилалтыг үл тоох;
2. уг тоо нь SET эсвэл SEQUENCE-ийн нэмэлт элемент болж байгаа тохиолдолд тоологдсон загварт ашиглагдаж буй ENUMERATED төрлийн эсвэл INTEGER төрлийн бүх үл мэдэгдэх нэртэй тоог үл тоох;
3. СОНГОЛТ нь өөрөө SET эсвэл SEQUENCE-ийн нэмэлт элемент болох СОНГОЛТ-д, SEQUENCE-ийн төгсгөлд эсвэл CHOICE-д үл мэдэгдэх бүх элементүүдийг үл тоох.

Хэрэв гэнэтийн утгыг агуулсан өргөтгөл нь чухал гэж тэмдэглэгдсэн бол хэрэгжилт нь хүлээн зөвшөөрөгдөөгүй өргөтгөлийг агуулсан гэрчилгээ эсвэл ХГЖ-аас ЗААВАЛ татгалзана.

ХАВСРАЛТ С: Жишээ

Энэхүү хавсралт нь гурван гэрчилгээний, нэг ХГЖ-ын жишээг агуулна. Эхний хоёр гэрчилгээ болон ХГЖ нь хамгийн бага баталгаажуулалтын шатлалтыг агуулдаг.

Хавсралт С.1-д ялгах нэр нь cn=Example CA,dc=example,dc=com гэж ГОБ- аар олгосон "өөрөө өөртөө гарын үсэг зурсан" гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Гэрчилгээ нь RSA нийтийн түлхүүрийг агуулах бөгөөд холбогдох RSA-ын хувийн түлхүүрээр гарын үсэг зурна.

Хавсралт С.2-д эцсийн объектын гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Эцсийн объектын гэрчилгээ нь RSA нийтийн түлхүүрийг агуулсан бөгөөд Хавсралт С.1 дэх "өөрөө өөртөө гарын үсэг зурсан" гэрчилгээнд тохирох хувийн түлхүүрээр гарын үсэг зурна.

Хавсралт С.3 нь параметр бүхий DSA нийтийн түлхүүрийг агуулсан, DSA болон SHA-1-ээр гарын үсэг зурсан эцсийн объектын гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Энэ гэрчилгээ нь хамгийн бага баталгаажуулалтын шатлалын нэг хэсэг биш юм.

Хавсралт С.4 нь ХГЖ- ын тэмдэглэсэн hex dump агуулдаг. ХГЖ-ыг ятгах нэр нь cn=Example CA,dc=example,dc=com гэж ГОБ-аас гаргадаг бөгөөд хүчингүй болсон гэрчилгээний жагсаалтад Хавсралт С.2-т үзүүлсэн эцсийн объектын гэрчилгээ багтсан болно.

Гаралтыг бий болгохын тулд Питер Гутманы dumpasn1 хэрэгслийг ашиглан гэрчилгээг боловсруулсан. dumpasn1 хэрэгслийг дараах холбоосоор авах боломжтой <http://www.cs.auckland.ac.nz/~pgut001/dumpasn1.c>. Гэрчилгээ болон ХГЖ-ын хоёртын файлыг дараах холбоосоор авах боломжтой http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/pkixtools.

Энэ хавсралтын хэсэгт тэмдэгт дүрслэлийг ашиглан ялгах нэрийг заасан газруудад тэмдэгтүүдийг [RFC4514]-д заасан дүрмийн дагуу форматална.

С.1. RSA өөрөө өөртөө гарын үсэг зурсан гэрчилгээ

Энэхүү хавсралт нь 578 байт 3-р хувилбарын гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Гэрчилгээ нь дараах мэдээллийг агуулна:

(a) the serial number is 17;

(b) the certificate is signed with RSA and the SHA-1 hash algorithm;

(c) the issuer's distinguished name is

cn=Example CA,dc=example,dc=com;

(d) the subject's distinguished name is cn=Example CA,dc=example,dc=com;

(e) the certificate was issued on April 30, 2004 and expired on April 30, 2005;

(f) the certificate contains a 1024-bit RSA public key;

(g) the certificate contains a subject key identifier extension generated using method (1) of Section 4.2.1.2; and

(h) the certificate is a CA certificate (as indicated through the basic constraints extension).

```
 0  574: SEQUENCE {
 4  423:   SEQUENCE {
 8    3:     [0] {
10    1:       INTEGER 2
      :       }
13    1:     INTEGER 17
16   13:     SEQUENCE {
18    9:       OBJECT IDENTIFIER
      :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
29    0:       NULL
      :       }
31   67:     SEQUENCE {
33   19:       SET {
35   17:         SEQUENCE {
37   10:           OBJECT IDENTIFIER
      :             domainComponent (0 9 2342 19200300 100 1 25)
49    3:           IA5String 'com'
      :           }
      :         }
54   23:       SET {
56   21:         SEQUENCE {
58   10:           OBJECT IDENTIFIER
      :             domainComponent (0 9 2342 19200300 100 1 25)
70    7:           IA5String 'example'
      :           }
      :         }
79   19:       SET {
81   17:         SEQUENCE {
```

```
 83   3:         OBJECT IDENTIFIER  commonName (2 5 4 3)
 88  10:         PrintableString 'Example CA'
     :       }
     :     }
     :   }
100  30:   SEQUENCE {
102  13:     UTCTime  30/04/2004  14:25:34 GMT
117  13:     UTCTime  30/04/2005  14:25:34 GMT
     :   }
132  67:   SEQUENCE {
134  19:     SET {
136  17:       SEQUENCE {
138  10:         OBJECT IDENTIFIER
     :           domainComponent (0 9 2342  19200300  100 1 25)
150   3:         IA5String 'com'
     :       }
     :     }
155  23:     SET {
157  21:       SEQUENCE {
159  10:         OBJECT IDENTIFIER
     :           domainComponent (0 9 2342  19200300  100 1 25)
171   7:         IA5String 'example'
     :       }
     :     }
180  19:     SET {
182  17:       SEQUENCE {
184   3:         OBJECT IDENTIFIER  commonName (2 5 4 3)
189  10:         PrintableString  'Example CA'
     :       }
     :     }
     :   }
201 159:   SEQUENCE {
204  13:     SEQUENCE {
206   9:       OBJECT IDENTIFIER
     :         rsaEncryption (1 2 840 113549  1 1 1)
217   0:       NULL
     :     }
219 141:     BIT STRING,  encapsulates {
223 137:       SEQUENCE {
226 129:         INTEGER
     :           00 C2 D7 97 6D 28 70 AA 5B CF 23 2E 80 70 39 EE
     :           DB 6F D5 2D D5 6A 4F 7A 34 2D F9 22 72 47 70 1D
     :           EF 80 E9 CA 30 8C 00 C4 9A 6E 5B 45 B4 6E A5 E6
     :           6C 94 0D FA 91 E9 40 FC 25 9D C7 B7 68 19 56 8F
     :           11 70 6A D7 F1 C9 11 4F 3A 7E 3F 99 8D 6E 76 A5
```

```
    :           74 5F 5E A4 55 53 E5 C7 68 36 53 C7 1D 3B 12 A6
    :           85 FE BD 6E A1 CA DF 35 50 AC 08 D7 B9 B4 7E 5C
    :           FE E2 A3 2C D1 23 84 AA 98 C0 9B 66 18 9A 68 47
    :           E9
358   3:         INTEGER 65537
    :         }
    :       }
    :     }
363  66:     [3] {
365  64:       SEQUENCE {
367  29:         SEQUENCE {
369   3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
374  22:           OCTET STRING, encapsulates {
376  20:             OCTET STRING
    :             08 68 AF 85 33 C8 39 4A 7A F8 82 93 8E 70 6A 4A
    :             20 84 2C 32
    :           }
    :         }
398  14:         SEQUENCE {
400   3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
405   1:           BOOLEAN TRUE
408   4:           OCTET STRING, encapsulates {
410   2:             BIT STRING 1 unused bits
    :             '0000011'B
    :           }
    :         }
414  15:         SEQUENCE {
416   3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
421   1:           BOOLEAN TRUE
424   5:           OCTET STRING, encapsulates {
426   3:             SEQUENCE {
428   1:               BOOLEAN TRUE
    :             }
    :           }
    :         }
    :       }
    :     }
    :   }
431  13:   SEQUENCE {
433   9:     OBJECT IDENTIFIER
    :       sha1withRSAEncryption (1 2 840 113549 1 1 5)
444   0:     NULL
    :   }
446 129:   BIT STRING
    :     6C F8 02 74 A6 61 E2 64 04 A6 54 0C 6C 72 13 AD
```

```
:    3C 47 FB F6 65 13 A9 85 90 33 EA 76 A3 26 D9 FC
:    D1 0E 15 5F 28 B7 EF 93 BF 3C F3 E2 3E 7C B9 52
:    FC 16 6E 29 AA E1 F4 7A 6F D5 7F EF B3 95 CA F3
:    66 88 83 4E A1 35 45 84 CB BC 9B B8 C8 AD C5 5E
:    46 D9 0B 0E 8D 80 E1 33 2B DC BE 2B 92 7E 4A 43
:    A9 6A EF 8A 63 61 B3 6E 47 38 BE E8 0D A3 67 5D
:    F3 FA 91 81 3C 92 BB C5 5F 25 25 EB 7C E7 D8 A1
:  }
```

C.2. RSA ашигласан эцсийн объектын гэрчилгээ

Энэхүү хавсралтад 629 байт 3-р хувилбарын гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Гэрчилгээ нь дараах мэдээллийг агуулна:

(a) the serial number is 18;

(b) the certificate is signed with RSA and the SHA-1 hash algorithm;

(c) the issuer's distinguished name is cn=Example CA,dc=example,dc=com;

(d) the subject's distinguished name is cn=End Entity,dc=example,dc=com;

(e) the certificate was valid from September 15, 2004 through March 15, 2005;

(f) the certificate contains a 1024-bit RSA public key;

(g) the certificate is an end entity certificate, as the basic constraints extension is not present;

(h) the certificate contains an authority key identifier extension matching the subject key identifier of the certificate in appendix C.1; and

(i) the certificate includes one alternative name- - an electronic mail address (rfc822Name) of "end.entity@example.com".

```
0  625: SEQUENCE {
4  474:   SEQUENCE {
8    3:     [0] {
```

```
 10   1:     INTEGER 2
      :     }
 13   1:    INTEGER 18
 16  13:    SEQUENCE {
 18   9:     OBJECT IDENTIFIER
      :     sha1withRSAEncryption (1 2 840 113549 1 1 5)
 29   0:     NULL
      :     }
 31  67:    SEQUENCE {
 33  19:     SET {
 35  17:      SEQUENCE {
 37  10:       OBJECT IDENTIFIER
      :       domainComponent (0 9 2342 19200300 100 1 25)
 49   3:       IA5String 'com'
      :      }
      :     }
 54  23:     SET {
 56  21:      SEQUENCE {
 58  10:       OBJECT IDENTIFIER
      :       domainComponent (0 9 2342 19200300 100 1 25)
 70   7:       IA5String 'example'
      :      }
      :     }
 79  19:     SET {
 81  17:      SEQUENCE {
 83   3:       OBJECT IDENTIFIER commonName (2 5 4 3)
 88  10:       PrintableString 'Example CA'
      :      }
      :     }
      :    }
100  30:    SEQUENCE {
102  13:     UTCTime 15/09/2004 11:48:21 GMT
117  13:     UTCTime 15/03/2005 11:48:21 GMT
      :    }
132  67:    SEQUENCE {
134  19:     SET {
136  17:      SEQUENCE {
138  10:       OBJECT IDENTIFIER
      :       domainComponent (0 9 2342 19200300 100 1 25)
150   3:       IA5String 'com'
      :      }
      :     }
155  23:     SET {
157  21:      SEQUENCE {
159  10:       OBJECT IDENTIFIER
```

```
    :           domainComponent (0 9 2342 19200300 100 1 25)
171   7:          IA5String 'example'
    :         }
    :       }
180  19:     SET {
182  17:       SEQUENCE {
184   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
189  10:         PrintableString 'End Entity'
    :         }
    :       }
    :     }
201 159:    SEQUENCE {
204  13:     SEQUENCE {
206   9:       OBJECT IDENTIFIER
    :         rsaEncryption (1 2 840 113549 1 1 1)
217   0:       NULL
    :       }
219 141:     BIT STRING, encapsulates {
223 137:       SEQUENCE {
226 129:         INTEGER
    :           00 E1 6A E4 03 30 97 02 3C F4 10 F3 B5 1E 4D 7F
    :           14 7B F6 F5 D0 78 E9 A4 8A F0 A3 75 EC ED B6 56
    :           96 7F 88 99 85 9A F2 3E 68 77 87 EB 9E D1 9F C0
    :           B4 17 DC AB 89 23 A4 1D 7E 16 23 4C 4F A8 4D F5
    :           31 B8 7C AA E3 1A 49 09 F4 4B 26 DB 27 67 30 82
    :           12 01 4A E9 1A B6 C1 0C 53 8B 6C FC 2F 7A 43 EC
    :           33 36 7E 32 B2 7B D5 AA CF 01 14 C6 12 EC 13 F2
    :           2D 14 7A 8B 21 58 14 13 4C 46 A3 9A F2 16 95 FF
    :           23
358   3:         INTEGER 65537
    :       }
    :     }
363 117:    [3] {
365 115:     SEQUENCE {
367  33:       SEQUENCE {
369   3:         OBJECT IDENTIFIER subjectAltName (2 5 29 17)
374  26:         OCTET STRING, encapsulates {
376  24:           SEQUENCE {
378  22:             [1] 'end.entity@example.com'
    :           }
    :         }
    :       }
402  29:       SEQUENCE {
404   3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
```

```
409  22:         OCTET STRING, encapsulates {
411  20:           OCTET STRING
     :             17 7B 92 30 FF 44 D6 66 E1 90 10 22 6C 16 4F C0
     :             8E 41 DD 6D
     :           }
     :         }
433  31:       SEQUENCE {
435   3:         OBJECT IDENTIFIER
     :           authorityKeyIdentifier (2 5 29 35)
440  24:         OCTET STRING, encapsulates {
442  22:           SEQUENCE {
444  20:             [0]
     :               08 68 AF 85 33 C8 39 4A 7A F8 82 93 8E 70 6A
     :               4A 20 84 2C 32
     :             }
     :           }
     :         }
466  14:       SEQUENCE {
468   3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
473   1:         BOOLEAN TRUE
476   4:         OCTET STRING, encapsulates {
478   2:           BIT STRING 6 unused bits
     :             '11'B
     :           }
     :         }
     :       }
     :     }
     :   }
482  13:   SEQUENCE {
484   9:     OBJECT IDENTIFIER
     :       sha1withRSAEncryption (1 2 840 113549 1 1 5)
495   0:     NULL
     :   }
497 129:   BIT STRING
     :     00 20 28 34 5B 68 32 01 BB 0A 36 0E AD 71 C5 95
     :     1A E1 04 CF AE AD C7 62 14 A4 1B 36 31 C0 E2 0C
     :     3D D9 1E C0 00 DC 10 A0 BA 85 6F 41 CB 62 7A B7
     :     4C 63 81 26 5E D2 80 45 5E 33 E7 70 45 3B 39 3B
     :     26 4A 9C 3B F2 26 36 69 08 79 BB FB 96 43 77 4B
     :     61 8B A1 AB 91 64 E0 F3 37 61 3C 1A A3 A4 C9 8A
     :     B2 BF 73 D4 4D E4 58 E4 62 EA BC 20 74 92 86 0E
     :     CE 84 60 76 E9 73 BB C7 85 D3 91 45 EA 62 5D CD
     :   }
```

C.3. DSA ашигласан эцсийн объектын гэрчилгээ

Энэ хавсралтад 914 байт 3-р хувилбарын гэрчилгээний тэмдэглэсэн hex dump агуулдаг. Гэрчилгээ нь дараах мэдээллийг агуулна:

a) Сериал дугаар 256 байна;

b) Гэрчилгээ нь DSA болон SHA-1 хэш алгоритмтай гарын үсэг зурсан;

c) the issuer's distinguished name is cn=Example DSA CA,dc=example,dc=com;

d) the subject's distinguished name is cn=DSA End Entity,dc=example,dc=com;

e) Гэрчилгээ нь 2004 оны 5-р сарын 2-нд олгогдсон бөгөөд 2005 оны 5- сарын 2-ны өдөр дууссан;

f) Гэрчилгээ нь параметр бүхий 1024 битийн DSA нийтийн түлхүүрийг агуулна;

g) Гэрчилгээ нь эцсийн объектын гэрчилгээ (ГОБ-ын гэрчилгээ биш);

h) the certificate includes a subject alternative name of "<http://www.example.com/users/DSAendentity.html>" and an issuer alternative name of "<http://www.example.com>"- - both are URLs;

i) Гэрчилгээ нь ГОБ-ын түлхүүрийн адилтгагч өргөтгөл болон OID 2.16.840.1.101.3.2.1.48.9 бодлогыг тодорхойлсон гэрчилгээний бодлогын өргөтгөл агуулсан

j) Энэхүү гэрчилгээ нь нийтийн түлхүүр нь тоон гарын үсгийг баталгаажуулахад зориулагдсан гэдгийг тодорхойлсон чухал түлхүүрийн хэрэглээний өргөтгөлийг агуулдаг.

```
 0  910: SEQUENCE {
 4  846:   SEQUENCE {
 8    3:     [0] {
10    1:       INTEGER  2
     :     }
13    2:     INTEGER  256
17    9:     SEQUENCE {
19    7:       OBJECT IDENTIFIER  dsaWithSha1 (1 2 840 10040 4 3)
     :     }
28   71:     SEQUENCE {
30   19:       SET {
32   17:         SEQUENCE {
34   10:           OBJECT IDENTIFIER
     :             domainComponent (0 9 2342 19200300 100 1 25)
46    3:           IA5String 'com'
     :         }
     :       }
```

```
 51  23:      SET {
 53  21:        SEQUENCE {
 55  10:          OBJECT IDENTIFIER
     :          domainComponent (0 9 2342 19200300 100 1 25)
 67   7:          IA5String 'example'
     :        }
     :      }
 76  23:      SET {
 78  21:        SEQUENCE {
 80   3:          OBJECT IDENTIFIER commonName (2 5 4 3)
 85  14:          PrintableString 'Example DSA CA'
     :        }
     :      }
     :    }
101  30:    SEQUENCE {
103  13:      UTCTime 02/05/2004 16:47:38 GMT
118  13:      UTCTime 02/05/2005 16:47:38 GMT
     :    }
133  71:    SEQUENCE {
135  19:      SET {
137  17:        SEQUENCE {
139  10:          OBJECT IDENTIFIER
     :          domainComponent (0 9 2342 19200300 100 1 25)
151   3:          IA5String 'com'
     :        }
     :      }
156  23:      SET {
158  21:        SEQUENCE {
160  10:          OBJECT IDENTIFIER
     :          domainComponent (0 9 2342 19200300 100 1 25)
172   7:          IA5String 'example'
     :        }
     :      }
181  23:      SET {
183  21:        SEQUENCE {
185   3:          OBJECT IDENTIFIER commonName (2 5 4 3)
190  14:          PrintableString 'DSA End Entity'
     :        }
     :      }
     :    }
206 439:    SEQUENCE {
210 300:      SEQUENCE {
214   7:        OBJECT IDENTIFIER dsa (1 2 840 10040 4 1)
223 287:        SEQUENCE {
227 129:          INTEGER
```

```
    :           00 B6 8B 0F 94 2B 9A CE A5 25 C6 F2 ED FC FB 95
    :           32 AC 01 12 33 B9 E0 1C AD 90 9B BC 48 54 9E F3
    :           94 77 3C 2C 71 35 55 E6 FE 4F 22 CB D5 D8 3E 89
    :           93 33 4D FC BD 4F 41 64 3E A2 98 70 EC 31 B4 50
    :           DE EB F1 98 28 0A C9 3E 44 B3 FD 22 97 96 83 D0
    :           18 A3 E3 BD 35 5B FF EE A3 21 72 6A 7B 96 DA B9
    :           3F 1E 5A 90 AF 24 D6 20 F0 0D 21 A7 D4 02 B9 1A
    :           FC AC 21 FB 9E 94 9E 4B 42 45 9E 6A B2 48 63 FE
    :           43
359  21:          INTEGER
    :           00 B2 0D B0 B1 01 DF 0C 66 24 FC 13 92 BA 55 F7
    :           7D 57 74 81 E5
382 129:          INTEGER
    :           00 9A BF 46 B1 F5 3F 44 3D C9 A5 65 FB 91 C0 8E
    :           47 F1 0A C3 01 47 C2 44 42 36 A9 92 81 DE 57 C5
    :           E0 68 86 58 00 7B 1F F9 9B 77 A1 C5 10 A5 80 91
    :           78 51 51 3C F6 FC FC CC 46 C6 81 78 92 84 3D F4
    :           93 3D 0C 38 7E 1A 5B 99 4E AB 14 64 F6 0C 21 22
    :           4E 28 08 9C 92 B9 66 9F 40 E8 95 F6 D5 31 2A EF
    :           39 A2 62 C7 B2 6D 9E 58 C4 3A A8 11 81 84 6D AF
    :           F8 B4 19 B4 C2 11 AE D0 22 3B AA 20 7F EE 1E 57
    :           18
    :         }
    :       }
514 132:      BIT STRING, encapsulates {
518 128:        INTEGER
    :         30 B6 75 F7 7C 20 31 AE 38 BB 7E 0D 2B AB A0 9C
    :         4B DF 20 D5 24 13 3C CD 98 E5 5F 6C B7 C1 BA 4A
    :         BA A9 95 80 53 F0 0D 72 DC 33 37 F4 01 0B F5 04
    :         1F 9D 2E 1F 62 D8 84 3A 9B 25 09 5A 2D C8 46 8E
    :         2B D4 F5 0D 3B C7 2D C6 6C B9 98 C1 25 3A 44 4E
    :         8E CA 95 61 35 7C CE 15 31 5C 23 13 1E A2 05 D1
    :         7A 24 1C CB D3 72 09 90 FF 9B 9D 28 C0 A1 0A EC
    :         46 9F 0D B8 D0 DC D0 18 A6 2B 5E F9 8F B5 95 BE
    :       }
    :     }
649 202:    [3] {
652 199:      SEQUENCE {
655  57:       SEQUENCE {
657   3:         OBJECT IDENTIFIER subjectAltName (2 5 29 17)
662  50:         OCTET STRING, encapsulates {
664  48:           SEQUENCE {
666  46:             [6]
    :               'http://www.example.com/users/DSAendentity.'
    :               'html'
```

```
    :           }
    :         }
    :       }
714  33:     SEQUENCE {
716   3:       OBJECT IDENTIFIER issuerAltName (2 5 29 18)
721  26:       OCTET STRING, encapsulates {
723  24:         SEQUENCE {
725  22:           [6] 'http://www.example.com'
    :           }
    :         }
    :       }
749  29:     SEQUENCE {
751   3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
756  22:       OCTET STRING, encapsulates {
758  20:         OCTET STRING
    :           DD 25 66 96 43 AB 78 11 43 44 FE 95 16 F9 D9 B6
    :           B7 02 66 8D
    :         }
    :       }
780  31:     SEQUENCE {
782   3:       OBJECT IDENTIFIER
    :         authorityKeyIdentifier (2 5 29 35)
787  24:       OCTET STRING, encapsulates {
789  22:         SEQUENCE {
791  20:           [0]
    :             86 CA A5 22 81 62 EF AD 0A 89 BC AD 72 41 2C
    :             29 49 F4 86 56
    :           }
    :         }
    :       }
813  23:     SEQUENCE {
815   3:       OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
820  16:       OCTET STRING, encapsulates {
822  14:         SEQUENCE {
824  12:           SEQUENCE {
826  10:             OBJECT IDENTIFIER '2 16 840 1 101 3 2 1 48 9'
    :           }
    :         }
    :       }
    :     }
838  14:     SEQUENCE {
840   3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
845   1:       BOOLEAN TRUE
848   4:       OCTET STRING, encapsulates {
850   2:         BIT STRING 7 unused bits
```

```
     :             '1'B (bit 0)
     :           }
     :         }
     :       }
     :     }
     :   }
 854   9:  SEQUENCE {
 856   7:    OBJECT IDENTIFIER dsaWithSha1 (1 2 840 10040 4 3)
     :   }
 865  47:  BIT STRING, encapsulates {
 868  44:    SEQUENCE {
 870  20:      INTEGER
     :       65 57 07 34 DD DC CA CC 5E F4 02 F4 56 42 2C 5E
     :       E1 B3 3B 80
 892  20:      INTEGER
     :       60 F4 31 17 CA F4 CF FF EE F4 08 A7 D9 B2 61 BE
     :       B1 C3 DA BF
     :     }
     :   }
     : }
```

C.4. Хүчингүй гэрчилгээний жагсаалт

Энэ хавсралт нь хоёр өргөтгөлтэй (cRLNumber and authorityKeyIdentifier) ХГЖ-ын хувилбар 2-ын тэмдэглэсэн hex dump агуулдаг. ХГЖ-ыг 2005 оны 2-р сарын 5-нд cn=Example CA,dc=example,dc=com гэж олгосон; дараагийн төлөвлөсөн олголт нь 2005 оны 2-р сарын 6. ХГЖ нь хүчингүй болсон нэг гэрчилгээг агуулдаг: сериалын дугаар 18, 2004 оны 11-р сарын 19-нд keyCompromise-ийн улмаас хүчингүй болсон. ХГЖ нь өөрөө 12 дугаартай бөгөөд RSA болон SHA-1-ээр гарын үсэг зурсан.

```
  0 352: SEQUENCE {
  4 202:   SEQUENCE {
  7   1:     INTEGER 1
 10  13:     SEQUENCE {
 12   9:       OBJECT IDENTIFIER
     :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
 23   0:       NULL
     :       }
 25  67:     SEQUENCE {
 27  19:       SET {
 29  17:         SEQUENCE {
 31  10:           OBJECT IDENTIFIER
     :             domainComponent (0 9 2342 19200300 100 1 25)
 43   3:           IA5String 'com'
     :         }
```

```
    :       }
 48  23:      SET {
 50  21:       SEQUENCE {
 52  10:        OBJECT IDENTIFIER
    :          domainComponent (0 9 2342 19200300 100 1 25)
 64   7:        IA5String 'example'
    :         }
    :       }
 73  19:      SET {
 75  17:       SEQUENCE {
 77   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
 82  10:        PrintableString 'Example CA'
    :         }
    :       }
    :     }
 94  13:   UTCTime 05/02/2005 12:00:00 GMT
109  13:   UTCTime 06/02/2005 12:00:00 GMT
124  34:   SEQUENCE {
126  32:     SEQUENCE {
128   1:      INTEGER 18
131  13:      UTCTime 19/11/2004 15:57:03 GMT
146  12:      SEQUENCE {
148  10:       SEQUENCE {
150   3:        OBJECT IDENTIFIER cRLReason (2 5 29 21)
155   3:        OCTET STRING, encapsulates {
157   1:         ENUMERATED 1
    :          }
    :         }
    :        }
    :       }
    :     }
160  47:   [0] {
162  45:     SEQUENCE {
164  31:      SEQUENCE {
166   3:       OBJECT IDENTIFIER
    :          authorityKeyIdentifier (2 5 29 35)
171  24:       OCTET STRING, encapsulates {
173  22:        SEQUENCE {
175  20:         [0]
    :          08 68 AF 85 33 C8 39 4A 7A F8 82 93 8E 70 6A
    :          4A 20 84 2C 32
    :         }
    :        }
    :       }
197  10:      SEQUENCE {
```

```
199    3:          OBJECT IDENTIFIER  cRLNumber (2 5 29 20)
204    3:          OCTET STRING, encapsulates {
206    1:            INTEGER  12
       :           }
       :         }
       :       }
       :     }
       :   }
209   13:   SEQUENCE {
211    9:     OBJECT IDENTIFIER
       :       sha1withRSAEncryption (1 2 840 113549 1 1 5)
222    0:     NULL
       :   }
224  129:   BIT STRING
       :     22 DC 18 7D F7 08 CE CC 75 D0 D0 6A 9B AD 10 F4
       :     76 23 B4 81 6E B5 6D BE 0E FB 15 14 6C C8 17 6D
       :     1F EE 90 17 A2 6F 60 E4 BD AA 8C 55 DE 8E 84 6F
       :     92 F8 9F 10 12 27 AF 4A D4 2F 85 E2 36 44 7D AA
       :     A3 4C 25 38 15 FF 00 FD 3E 7E EE 3D 26 12 EB D8
       :     E7 2B 62 E2 2B C3 46 80 EF 78 82 D1 15 C6 D0 9C
       :     72 6A CB CE 7A ED 67 99 8B 6E 70 81 7D 43 42 74
       :     C1 A6 AF C1 55 17 A2 33 4C D6 06 98 2B A4 FC 2E
       :   }
```

Зохиогчдын хаяг

David Cooper
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA
EMail: david.cooper@nist.gov

Stefan Santesson
Microsoft
One Microsoft Way
Redmond, WA 98052
USA
EMail: stefans@microsoft.com

Stephen Farrell

Distributed Systems Group
Computer Science Department
Trinity College Dublin
Ireland
EMail: stephen.farrell@cs.tcd.ie

Sharon Boeyen
Entrust
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
EMail: sharon.boeyen@entrust.com

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
EMail: housley@vigilsec.com

Tim Polk
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA
EMail: wpolk@nist.gov

Оюуны өмчийн эрх

IETF нь энэхүү баримт бичигт дурдсан технологийг хэрэгжүүлэх, ашиглахтай холбоотой Оюуны өмчийн эрх болон бусад эрхийн хүчин төгөлдөр байдал, хамрах хүрээ, мөн иймэрхийндагуу ямар нэгэн лиценз байж болох, үгүй байж болох талаар байр сууриа илэрхийлдэггүй; мөн иймэрхийг тодорхойлохын тулд бие даасан хүчин чармайлт гаргаагүй. RFC баримт бичигт хамаарах эрхийн журмын талаарх мэдээллийг BCP 78 болон BCP 79-ээс олж болно.

IETF-ийн Нарийн бичгийн дарга нарын газарт хийсэн оюуны өмчийн эрхийн ил тод байдлын хуулбар болон лицензийн талаарх аливаа баталгаа, эсвэл ерөнхий лиценз авах оролдлого, эсвэл энэ тодорхойлолтыг хэрэгжүүлэгчид эсвэл хэрэглэгчид ийм өмчийн эрхийг ашиглах зөвшөөрлийг http://www.ietf.org/ipr хаягаар IETF онлайн IPR дижитал сангаас авч болно.

IETF нь энэхүү стандартыг хэрэгжүүлэхэд шаардагдах технологид хамаарах аливаа зохиогчийн эрх, патент, патентын мэдүүлэг болон бусад өмчийн эрхэд дурын сонирхогч тал анхаарлаа хандуулахыг санал болгож байна. IETF-ийн ietf-ipr@ietf.org хаягаар хандаж мэдээлэл авна уу.