**Списки відкликаних сертифікатів (CRL)**

Ці списки періодично оновлюються. На скільки переодично, це заклається регламентом центру сертицікації.

**CRL – Certificate Revocation List**

Кожен список фіксує інформацію, що видається центром сертицкацєї.

* Розглядаються тільки сертифікати, які на поточний момент часу чинні за сроками дії
* Тількі заблоковані або відкриті сертифікати .Якщо у сертифікату вийшов термін дії, то він виключається зі списку відкликаних сертифікатів, якщо його було перед цим відкликано. Якщо сертифікат заблоковано, то він з’являється у певному списку відкритих сертифікатів, а потім коли його буде поновлено, він виключається зі списку, тобто він буде фігурувати тільки на той час, коли його було заблоковано і все. Після чого він зникає та одержує автоматом статус **дійсний.**

У інтервал часу публікування відкладених сертифікатів статус сертифікатів не може бути змінений.

Якщо ви кориневий центр сертифікації України, то вам нема потреби кожну добу випускати новий список сертифікатів, бо імовірність того, що сертифікат потрібно буде відкликати дуже мала.

Існує уточнення механізму **CRL.**

Ми не хочемо публікувати новий список, бо він великий, але статуси потрібно оперативно оновлювати, тому будемо опубліковувати малесенький списочок о том, що саме змінилося після останньої публікації списку відкладених. Ці списки звуться **дельта-списками**. Вони маленькі бо описують статус не усіх сертиікатів, а тих, для яких відбулась зміна статусу після останнього списку відкладенних сертифікатів.

Формат CRL доведено у профілі сертифікатів **RFC5280**.

Список підписаних сертифікатів –ц е стандартная підписана структура

Sequence > Тіло – алгоритм підпису- підпис

Тіло TBSCErtList cкладається з наступних полів:

1. Version. За форматом стоїть опціональна, за помовченням версія 1, але наразі усі реалізації повинні використовувати списки версії 2
2. Копія поля з алгоритму підпису
3. Видавець списку відкликаних сертифікатів, зазвичай це той самий центр сертифікації, який сертифікати публікує
4. Час публікації списку відкладених сертифікатів .. Усі статсу фіксуються на цей час.
5. Час публікації наступного списку відкликаних сертифікатів. Український центр сертифікації вимагає наявність цього поля.
6. revokeCert

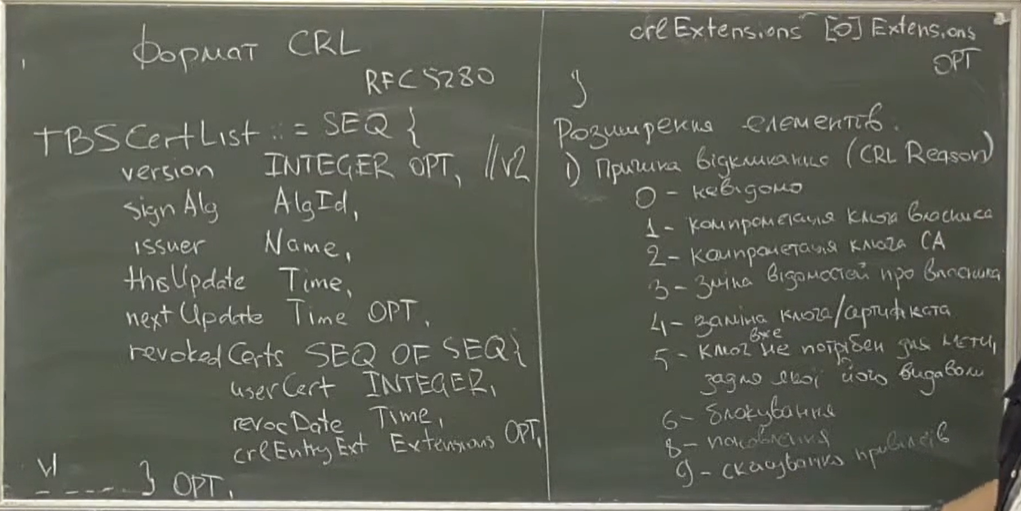
якщо усіх сертифікатів чинний статус, то це поле просто виключається зі списку, публікується порожній список.

1. Розширення власного списку відкладених сертифікатів

Розширення елементів

1. Причина відкликання (CRL Reason):

* Незрозуміло що
* Компрометація ключа власника сертифікату
* Зміна відомостей про власника
* Заміна ключа штатна, наприклад ключ користувач змінив
* Ключ вже не потрібен для мети, заради якої його видавали
* Блокування сертифікату
* Оновлення сертифікату – ця причина не використовується у головних списках відкликаних сертифікатів. Якщо сертифікат поновлено, то від виключається зі списку відкликаних сертифікатів, але ця причина використовується у дельта-списках.
* Відклик привілеїв(скасування) – для атрибутів сертифікатів, його відкликають, тому що для привилеї забрали у користовуча
* Компроментація атрибутного центру.



1. **Invalidity time** – час, коли стало відомо, що с ключем сертифікату, який відкликали стало щось негаразд. Це розширення несе тільки інформаційний характер

Розширення самого списку

1. Authority key Identifier
2. CRL Distribution Point – точка доступу
3. Freshest CRL – точка доступу до дельт, де найновіша інформація
4. CRL Number – серійний номер

Якщо центр сертифікації не підтримує дельта-списки, то усі списки, які вони публікують, повинні мати послідовні номери. Якщо центр підтримує дельта-списки, то усі списки відкликаних, які видає центр, будуть послідовні

1. Delta CRLIndicator – значення цього розширення – серійний номер, до якого цей дель-сертифікат відноситься

**Зауваження:**

1)Центр сертифікації може використовувати декілька списків в залежності від того, де їх затосовано.

* Тільки для сертифікатів користувачів
* Для сертифікатів центру сертифікації
* Для атрибутних сертифікатів
* Для деяих причин відкликання

2)CA може делегувати повноваження по формулюванню CRL ( indirect CRL). Непрямий, бо ви запрошуєте статус у СА, а повертає його зовсім інша структура.

- у Issue Distribution Point вказується галочка, що сертифікат непрямий

- у розширення елементу додається Certificate Issuer

