

ПОГОДЖЕНО
Заступник Голови Державної служби спеціального зв'язку та захисту інформації України

В. Корнейко

“ 12 ” 09 2013 р.



ЗАТВЕРДЖУЮ
Міністр Інформаційно-довідкового департаменту Міндоходів зборів України

О.В. Клименко

“ 12 ” 2013 р.



РЕГЛАМЕНТ

Акредитованого центру сертифікації ключів
Інформаційно-довідкового департаменту
Міндоходів
(Нова редакція)

ПОГОДЖЕНО
Начальник Управління (центру) сертифікації ключів Інформаційно-довідкового департаменту Міндоходів

О.Ю. Матвеев

“ 02 ” 09 2013 р.

ПОГОДЖЕНО
Директор Інформаційно-довідкового департаменту Міндоходів

Л. Романов

“ 03 ” 09 2013 р.



ЗМІСТ

1	ЗАГАЛЬНІ ПОЛОЖЕННЯ	4
1.1.	Ідентифікаційні дані АЦСК ІДД Міндоходів.....	4
1.2.	Визначення термінів.....	4
1.3.	Порядок внесення змін та доповнень до Регламенту.....	5
2	ПЕРЕЛІК СУБ'ЄКТІВ, ЗАДІЯНИХ В ОБСЛУГОВУВАННІ І ВИКОРИСТАННІ СЕРТИФІКАТІВ КЛЮЧІВ ТА ЇХ ФУНКЦІЇ.....	5
2.1.	Перелік суб'єктів.....	5
2.2.	АЦСК ІДД Міндоходів	5
2.3.	Послуги ЕЦП, які надає АЦСК ІДД Міндоходів.....	5
2.4.	Відокремлені пункти реєстрації.....	6
2.5.	Підписувачі та користувачі.....	6
3	СФЕРА ВИКОРИСТАННЯ СЕРТИФІКАТА КЛЮЧА.....	6
3.1.	Перелік сфер, у яких дозволяється використання сертифікатів ключів.....	6
3.2.	Обмеження щодо використання сертифікатів ключів.....	6
4	ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ АЦСК ІДД МІНДОХОДІВ.....	6
4.1.	Інформаційний ресурс АЦСК ІДД Міндоходів	6
4.2.	Порядок публікації сертифікату АЦСК ІДД Міндоходів та сертифікатів серверів АЦСК ІДД Міндоходів	7
4.3.	Порядок публікації посиленних сертифікатів ключів підписувачів	7
4.4.	Порядок публікації списків відкликаних сертифікатів.....	7
5	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ.....	7
5.1.	Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається для сертифікації.....	7
5.2.	Порядок ідентифікації та реєстрації заявників.....	7
5.3.	Ідентифікація та реєстрація юридичної особи.....	8
5.4.	Ідентифікація та реєстрація фізичної особи (фізичної особи - підприємця).....	8
5.5.	Порядок повторної реєстрації заявника після закінчення строку обслуговування посиленого сертифікату ключа.....	9
5.6.	Внесення змін до реєстраційних даних заявника (підписувача) або позапланова заміна посиленних сертифікатів ключів.....	10
5.7.	Автентифікація підписувача під час звернення щодо блокування, скасування та поновлення посиленого сертифіката ключа.....	10
5.8.	Захист персональних даних підписувачів.....	10
6	ПРОЦЕДУРИ ТА МЕХАНІЗМИ ОБСЛУГОВУВАННЯ ПОСИЛЕНИХ СЕРТИФІКАТІВ КЛЮЧІВ.....	10
6.1.	Порядок генерації ключів підписувачів.....	10
6.2.	Порядок подання запиту на сертифікацію.....	11
6.3.	Порядок формування сертифікатів та надання їх абонентам.....	11
6.4.	Порядок повторного формування сертифікату ключа.....	11
6.5.	Використання посиленого сертифіката та особистого ключа.....	12
6.6.	Підстави та порядок скасування, блокування та поновлення посиленних сертифікатів ключів.....	13
6.6.1.	Підстави та порядок скасування сертифікатів ключів підписувачів.....	13
6.6.2.	Обставини, за яких сертифікат повинен бути скасований заявником.....	13
6.6.3.	Порядок скасування посиленних сертифікатів ключів.....	13

6.6.4.	Порядок блокування посилених сертифікатів ключів.....	14
6.6.5.	Блокування посиленого сертифіката за заявою в усній формі.....	14
6.6.6.	Блокування посиленого сертифіката за заявою у письмовій формі.....	14
6.6.7.	Блокування посиленого сертифіката ключа за електронним запитом.....	14
6.6.8.	Порядок поновлення чинності посилених сертифікатів ключів.....	14
6.7.	Закінчення строку чинності посиленого сертифіката ключа підписувача	15
6.8.	Розповсюдження інформації про статус сертифікатів ключів.....	15
6.9.	Порядок надання послуг визначення статусу сертифіката в інтерактивному режимі (он-лайн перевірки статусу сертифікату).....	15
7	УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ.....	16
7.1.	Фізичне середовище.....	16
7.2.	Програмно-технічний комплекс АЦСК ІДД Міндоходів	16
7.3.	Пропускний і внутрішній режим.....	18
7.4.	Перелік конфіденційної та відкритої інформації, що обробляється в АЦСК ІДД Міндоходів	19
7.5.	Ведення журналів аудиту автоматизованої системи АЦСК ІДД Міндоходів.....	19
7.6.	Порядок ведення архівів та зберігання документованої інформації	19
7.7.	Організаційна структура АЦСК ІДД Міндоходів	20
7.7.1.	Підрозділ реєстрації.....	20
7.7.2.	Підрозділ безпеки, захисту інформації та адміністрування ПТК.....	21
7.7.3.	Підрозділ організаційно-методологічного забезпечення.....	22
7.7.4.	Відокремлені пункти реєстрації.....	22
7.7.5.	Функціональні обов'язки посадових осіб безпосередньо пов'язаних з обслуговуванням посилених сертифікатів ключів.....	22
8	ОПИС ПРОЦЕДУР ТА МЕХАНІЗМІВ, ПОВ'ЯЗАНИХ З ФУНКЦІОНУВАННЯМ АЦСК ІДД МІНДОХОДІВ.....	24
8.1.	Управління ключами АЦСК ІДД Міндоходів.....	24
8.1.1.	Порядок генерації та резервного копіювання особистого ключа АЦСК ІДД Міндоходів	24
8.1.2.	Управління ключами серверів АЦСК ІДД Міндоходів.....	25
8.1.3.	Порядок використання (введення) особистого ключа АЦСК ІДД Міндоходів.....	26
8.1.4.	Порядок планової зміни ключів АЦСК ІДД Міндоходів	26
8.1.5.	Порядок позапланової зміни ключів АЦСК ІДД Міндоходів	26
8.2.	Порядок надання послуги фіксування часу	27
8.3.	Порядок синхронізації часу у ПТК АЦСК ІДД Міндоходів	27

1. Загальні положення

Регламент Акредитованого центру сертифікації ключів Інформаційно-довідкового департаменту Міндоходів (далі – Регламент) визначає організаційні, технічні та інші умови діяльності Акредитованого центру сертифікації ключів Інформаційно-довідкового департаменту Міндоходів (далі – АЦСК ІДД Міндоходів) при наданні послуг електронного цифрового підпису (далі – ЕЦП).

Регламент розроблено з урахуванням норм та положень:

Закону України “Про електронний цифровий підпис” від 22.05.2003 року №852-IV;

постанов Кабінету Міністрів України:

від 26 травня 2004 року №680 «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу»;

від 13 липня 2004 року №903 «Про затвердження Порядку акредитації центру сертифікації ключів»;

Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 №3, зареєстрованих в Міністерстві юстиції України 27.01.2005 за №104/10384, у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 №50, зареєстрованого в Міністерстві юстиції України 17.05.2006 за №568/12442;

Наказу Міністерства юстиції України, Адміністрації державної служби спеціального зв'язку та захисту інформації від 20.08.2012 №1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 20 серпня 2012 року за №1398/21710 (із змінами);

Формати, структура та протоколи, що застосовуються під час формування та використання посилених сертифікатів власних відкритих ключів АЦСК ІДД Міндоходів, формування сертифікатів ключів абонентів, формування списків відкликаних сертифікатів абонентів, відповідають вимогам наказу Міністерства юстиції України, Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 №1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 20 серпня 2012 року за №1398/21710 (із змінами).

1.1. Ідентифікаційні дані АЦСК ІДД Міндоходів

Акредитований центр сертифікації ключів є структурним підрозділом Інформаційно-довідкового департаменту Міндоходів (код ЄДРПОУ 38725930) та розміщується за адресою м. Київ, Львівська пл., 8.

Контактний телефон ЦСК +38 (044) 284-00-10

Електронна поштова скринька (e-mail): inform@acskidd.gov.ua

Електронна адреса інформаційного ресурсу (веб-сайту): <http://www.acskidd.gov.ua>.

Норми цього Регламенту поширюються на:

- АЦСК ІДД Міндоходів;
- відокремлені пункти реєстрації заявників АЦСК ІДД Міндоходів (далі – Відокремлені пункти реєстрації);
- юридичних осіб публічного та приватного права, фізичних осіб – суб'єктів підприємницької діяльності, фізичних осіб – громадян України, осіб без громадянства, іноземців, які звернулись у встановленому Регламентом порядку до АЦСК ІДД Міндоходів чи його відокремлених пунктів реєстрації з метою отримання послуги ЕЦП або є його абонентами.

Чітке дотримання та виконання умов Регламенту для вищевказаних осіб є обов'язковим.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в АЦСК ІДД Міндоходів та у його відокремлених пунктах реєстрації.

1.2. Визначення термінів

У цьому Регламенті терміни вживаються у такому значенні:

заявник – фізична або юридична особа, яка звернулася у встановленому цим Регламентом порядку до АЦСК ІДД Міндоходів чи його відокремлених пунктів з метою отримання послуги ЕЦП;

абонент – особа, яка на законних підставах отримує від АЦСК ІДД Міндоходів послуги ЕЦП;

підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає ЕЦП під час створення електронного документа;

користувач – особа, яка використовує надійні засоби ЕЦП та дані про статус сертифікатів ключів для перевірки ЕЦП. Користувач може не бути абонентом АЦСК ІДД Міндоходів;

Інші терміни та визначення, що вживаються в цьому Регламенті, визначені наведеними вище нормативними актами.

1.3. Порядок внесення змін та доповнень до Регламенту

Внесення змін та доповнень до Регламенту здійснюється АЦСК ІДД Міндоходів у відповідності до чинного законодавства України.

Зміни та доповнення до Регламенту оприлюднюються на офіційному веб-сайті АЦСК ІДД Міндоходів.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту розміщення зазначених змін і доповнень на електронному інформаційному ресурсі АЦСК ІДД Міндоходів.

Зміни та доповнення внесені до Регламенту у зв'язку зі зміною законодавства України, набувають чинності одночасно із набранням чинності змін до відповідних нормативно-правових актів.

Договори, умови яких суперечать змінам чи доповненням до Регламенту, повинні бути переукладені протягом 10 (десяти) робочих днів з дня набрання чинності такими змінами.

2. Перелік суб'єктів, задіяних в обслуговуванні і використанні сертифікатів ключів та їх функції

2.1. Перелік суб'єктів

В обслуговуванні і використанні сертифікатів ключів АЦСК ІДД Міндоходів задіяні наступні суб'єкти:

- АЦСК ІДД Міндоходів, в тому числі відокремлені пункти реєстрації;
- підписувачі;
- користувачі.

2.2. АЦСК ІДД Міндоходів

АЦСК ІДД Міндоходів здійснює свою діяльність в сфері надання послуг ЕЦП органам державної влади, органам місцевого самоврядування, підприємствам, установам та організаціям всіх форм власності, іншим суб'єктам господарської діяльності та фізичним особам, з можливістю безоплатної видачі посилених сертифікатів відкритих ключів.

АЦСК ІДД Міндоходів не здійснює діяльність пов'язану з використанням інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

АЦСК ІДД Міндоходів надає послуги ЕЦП та здійснює діяльність на підставі свідоцтва про акредитацію.

Під послугами електронного цифрового підпису розуміється надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і заблокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України від 22.05.2003 року N 852-IV "Про електронний цифровий підпис".

Заявники мають право отримати в АЦСК ІДД Міндоходів посилені сертифікати відкритих ключів.

2.3. Послуги ЕЦП, які надає АЦСК ІДД Міндоходів

- 2.3.1. реєстрація заявників;
- 2.3.2. надання у користування надійних засобів ЕЦП;
- 2.3.3. допомога при генерації відкритих та особистих ключів;
- 2.3.4. обслуговування посилених сертифікатів ключів заявників, що включає:
 - 2.3.4.1. сертифікацію відкритих ключів заявників;
 - 2.3.4.2. розповсюдження та зберігання посилених сертифікатів ключів;
 - 2.3.4.3. управління статусом посилених сертифікатів ключів та розповсюдження інформації про статус сертифікатів ключів;
- 2.3.5. надання послуги фіксування часу;
- 2.3.6. консультативні послуги за зверненням підписувачів.

Надання зазначених послуг здійснюється відповідно до Регламенту та на підставі укладених договорів або договорів приєднання, укладених шляхом прийняття заяви приєднання.

2.4. Відокремлені пункти реєстрації

Відокремлені пункти реєстрації заявників – підрозділи АЦСК ІДД Міндоходів при територіальних органах Міндоходів, що реалізують функції з реєстрації заявників та їх подальшого обслуговування на відповідній території.

Відокремлені пункти діють на підставі Положення про Інформаційно-довідковий департамент Міндоходів, Регламенту Інформаційно-довідкового департаменту Міндоходів, Положення про АЦСК ІДД Міндоходів та власних положень, затверджених в установленому порядку, а щодо надання послуг ЕЦП на підставі Регламенту.

Відокремлені пункти уповноважені укладати договори про надання послуг ЕЦП від імені Інформаційно-довідкового департаменту Міндоходів.

Безпосереднє управління відокремленими пунктами здійснюється начальником (керівником) АЦСК ІДД Міндоходів.

2.5. Підписувачі та користувачі

Використовувати послуги АЦСК ІДД Міндоходів мають право як підписувачі так і користувачі.

Підписувачі користуються усім переліком послуг АЦСК ІДД Міндоходів на підставі укладеного договору (договору приєднання) та Регламенту.

Користувачі, які хоч і не знаходяться у договірних відносинах з АЦСК ІДД Міндоходів, але можуть використовувати надійні засоби ЕЦП для перевірки підпису або статусу сертифікатів, а також мають право використовувати інші послуги АЦСК ІДД Міндоходів, що не потребують автентифікації.

3. Сфера використання сертифіката ключа

3.1. Перелік сфер, у яких дозволяється використання сертифікатів ключів

Посилені сертифікати ключів, сформовані АЦСК ІДД Міндоходів, використовуються для засвідчення чинності і належності відкритого ключа підписувачу.

АЦСК ІДД Міндоходів здійснює обслуговування посиленних сертифікатів ключів, сформованих для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій всіх форм власності, фізичних осіб, незалежно від сфери їх використання.

Сферою використання посиленних сертифікатів АЦСК ІДД Міндоходів є організація електронного документообігу з використанням ЕЦП.

3.2. Обмеження щодо використання посиленних сертифікатів ключів

АЦСК ІДД Міндоходів має право встановлювати обмеження сфери використання сформованих ним посиленних сертифікатів ключів. Інформація щодо обмеження сфери використання доводиться до заявника (підписувача) та зазначається у сформованому АЦСК ІДД Міндоходів посиленому сертифікаті ключа.

4. Порядок розповсюдження (публікації) інформації АЦСК ІДД Міндоходів

4.1. Інформаційний ресурс АЦСК ІДД Міндоходів

Інформаційний ресурс АЦСК ІДД Міндоходів призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

- довідкову інформацію (режими роботи АЦСК ІДД Міндоходів та його відокремлених пунктів реєстрації, перелік та реквізити відокремлених пунктів реєстрації, положення Регламенту, Положення про Інформаційно-довідковий департамент Міндоходів, Положення про АЦСК ІДД Міндоходів, положення про відокремлені пункти реєстрації або витяги з них, нормативні документи, договори на надання послуг, форми заяв тощо);
- сертифікат АЦСК ІДД Міндоходів;
- сертифікати серверів АЦСК ІДД Міндоходів;
- посилені сертифікати абонентів;
- списки відкликаних сертифікатів, що містять інформацію про статуси сертифікатів АЦСК ІДД Міндоходів та абонентів.

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу: <http://www.acskidd.gov.ua>.

Технічною основою інформаційного ресурсу АЦСК ІДД Міндоходів є сервери взаємодії, що входять до складу програмно-технічного комплексу АЦСК ІДД Міндоходів.

Довідкова інформація розміщується на HTTP-сервері сервера взаємодії у вигляді набору web-сторінок.

Сертифікат АЦСК ІДД Міндоходів, сертифікати серверів АЦСК ІДД Міндоходів та абонентів, а також списки відкликаних сертифікатів розміщуються:

- у складі web-сторінок на HTTP-сервері сервера взаємодії;

- у інформаційному дереві LDAP-каталогу на LDAP-сервері сервера взаємодії.

Доступ до HTTP-сервера здійснюється за DNS-ім'ям <http://www.acskidd.gov.ua> за протоколом HTTP (номер TCP-порта 80).

Доступ до LDAP-сервера здійснюється за DNS-ім'ям <http://www.acskidd.gov.ua> за протоколом LDAP (номер TCP-порта 389).

4.2. Порядок публікації сертифікату АЦСК ІДД Міндоходів та сертифікатів серверів АЦСК ІДД Міндоходів

Після формування сертифікату АЦСК ІДД Міндоходів виконується його публікація на інформаційний ресурс. Окрім власного сертифіката АЦСК ІДД Міндоходів виконується публікація сертифікатів серверів АЦСК ІДД Міндоходів:

- сервера обробки запитів (CMP-сервера);
- сервера позначок часу (TSP-сервера);
- сервера визначення статусу сертифікатів (OCSP-сервера).

Публікація сертифікатів серверів АЦСК ІДД Міндоходів виконується після формування сертифіката відповідного сервера.

4.3. Порядок публікації посиленних сертифікатів підписувачів

Публікація посиленних сертифікатів підписувачів на інформаційному ресурсі АЦСК ІДД Міндоходів здійснюється за їх згодою. Інформація про необхідність публікації кожного окремого посиленого сертифікату вноситься у склад реєстраційних даних під час реєстрації заявника.

Публікація посиленних сертифікатів абонентів у інформаційному дереві LDAP-каталогу здійснюється автоматично з інтервалом синхронізації п'ятнадцять (15) хв.

4.4. Порядок публікації списків відкликаних сертифікатів

Публікація списків відкликаних сертифікатів абонентів на інформаційному ресурсі АЦСК ІДД Міндоходів (на HTTP-сервері) здійснюється одразу після його випуску.

АЦСК ІДД Міндоходів виконує випуск списків відкликаних сертифікатів двох типів:

- повний список;
- частковий список.

Повний список випускається один (1) раз на тиждень та містить інформацію про всі відкликані сертифікати, які були сформовані АЦСК ІДД Міндоходів на діючому особистому ключі.

Частковий список випускається кожні дві (2) години та містить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку.

Публікація списків відкликаних сертифікатів у інформаційному дереві LDAP-каталогу здійснюється автоматично з інтервалом синхронізації п'ять (5) хв.

5. Ідентифікація та автентифікація

5.1. Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається для сертифікації

Відкритий ключ заявника (підписувача) подається на сертифікацію виключно у вигляді самопідписаного запиту, який засвідчується ЕЦП за допомогою відповідного йому особистого ключа. Підтвердження володіння заявником (підписувачем) відповідним особистим ключем здійснюється без розкриття його особистого ключа, шляхом перевірки ЕЦП на запиті за допомогою відкритого ключа, що міститься у запиті.

5.2. Порядок ідентифікації та реєстрації заявників

Реєстрація заявника – це встановлення особи заявника, підписувача (підписувачів), перевірка наданих заявником даних, що включаються у сертифікат та внесення інформації про заявника та підписувача (підписувачів) до реєстру підписувачів АЦСК ІДД Міндоходів.

Заявник може бути представлений довіреною особою, якщо немає можливості його особистої присутності в АЦСК ІДД Міндоходів. У цьому випадку заявник надає довіреність на подання документів для реєстрації.

Довіреність засвідчується:

- для юридичних осіб: підписом керівника з прикладенням печатки організації;

- для фізичних осіб - підприємців – підписом підприємця з прикладенням його печатки або у разі відсутності печатки – нотаріально;
- для фізичних осіб – нотаріально.

Заявник (довірена особа) повинен ознайомитися із умовами обслуговування сертифікатів ключів, передбачених політикою сертифікації АЦСК ІДД Міндоходів, а також Регламентом.

Реєстрація здійснюється в присутності заявника або його довіреної особи.

5.3. Ідентифікація та реєстрація юридичної особи

Встановлення заявника – юридичної особи здійснюється за установчими документами юридичної особи або копіями таких документів, які нотаріально засвідчені відповідно до законодавства.

При ідентифікації юридичної особи з'ясовують:

- її повне найменування;
- місцезнаходження;
- відомості про органи управління та їх склад;
- дані, що ідентифікують осіб, які мають право розпоряджатися рахунками та майном, їх повноваження;
- ідентифікаційний код згідно з Єдиним державним реєстром юридичних осіб та фізичних осіб – підприємців.

Крім цього, під час реєстрації встановлюється представник юридичної особи та його повноваження.

Під час реєстрації уповноважена особа заявника (довірена особа) надає такі документи:

- заповнена та підписана заява на реєстрацію для отримання посиленого сертифіката ключа встановленого зразку та дозвіл на використання персональних даних підписувача для реєстрації підписувача у реєстрі підписувачів АЦСК ІДД Міндоходів та формування посиленого сертифікату відкритого ключа;
- оригінал статуту юридичної особи (положення про установу, філію) або його нотаріально засвідчену копію (*надається виключно для ознайомлення*);
- документи, що підтверджують повноваження керівника заявника (копія наказу про призначення тощо);
- документи, що підтверджують належність підписувача до юридичної особи – заявника та його повноваження, засвідчені печаткою та особистим підписом керівника юридичної особи;
- копії паспортів заявника та підписувачів (копії 1-4 сторінок), засвідчені власноручними підписами власників паспортів.
- копія облікової картки платника податків* (довідки про присвоєння ідентифікаційного коду ДРФО керівника та головного бухгалтера) у разі, якщо формується сертифікати для керівника та бухгалтера;

* - у разі, якщо через релігійні переконання фізична особа відмовилась від ідентифікаційного коду, копія облікової картки платника податків не подається.

Копії та витяги, крім нотаріально засвідчених, засвідчуються підписом керівника та печаткою юридичної особи, а також підписом уповноваженої особи ЦСК якій пред'являються копії разом з оригіналами. Використання факсимільного підпису при завірянні документів не допускається.

5.4. Ідентифікація та реєстрація фізичної особи (фізичної особи - підприємця)

Встановлення фізичної особи здійснюється за паспортом (або іншим документом, який засвідчує особу відповідно до законодавства України).

Під час реєстрації заявник (фізична особа) надає такі документи:

- заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразку;
- паспорт або копію паспорту заявника (копії 1-4 сторінок), засвідчену власноручним підписом власника;
- копія облікової картки платника податків (довідки про присвоєння ідентифікаційного коду ДРФО).*

Встановлення фізичної особи – підприємця здійснюється за паспортом.

Під час реєстрації заявник (фізична особа-підприємець) надає такі документи:

- заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразку та дозвіл на використання персональних даних підписувача для реєстрації підписувача у

реєстрі підписувачів АЦСК ІДД Міндоходів та формування посиленого сертифікату відкритого ключа;

- паспорт або копію паспорта заявника (копії 1-4 сторінок), засвідчену власноручним підписом власника;
- копія облікової картки платника податків (довідки про присвоєння ідентифікаційного коду ДРФО).*

При ідентифікації фізичної особи з'ясовують:

- прізвище, ім'я та по батькові;
- дату народження;
- серію і номер паспорта (або іншого документа, який засвідчує особу), дату видачі та орган, що його видав;
- ідентифікаційний код за ДРФО або відмітка в паспорті, у разі, якщо фізична особа через релігійні переконання відмовилась від ідентифікаційного коду.

* - у разі, якщо через релігійні переконання фізична особа відмовилась від ідентифікаційного коду, копія облікової картки платника податків не подається.

Копії та витяги, крім нотаріально засвідчених, засвідчуються підписом фізичної особи (підписом фізичної особи - підприємця та його печаткою, у разі її наявності), а також підписом уповноваженої особи АЦСК ІДД Міндоходів якій пред'являються копії разом з оригіналами. Використання факсимільного підпису при завірянні документів не допускається.

До розгляду не приймаються документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати.

Бланки реєстраційних документів (договір та заява приєднання, заява на реєстрацію, довіреність, тощо) встановленої форми розміщуються на інформаційному ресурсі АЦСК ІДД Міндоходів.

Адміністратор реєстрації АЦСК ІДД Міндоходів або віддалений адміністратор реєстрації виконує процедуру ідентифікації заявника (його довіреної особи), що проходить процедуру реєстрації, шляхом установлення особи за паспортом або іншим документом, що засвідчує особу.

Після позитивної ідентифікації адміністратор реєстрації АЦСК ІДД Міндоходів або віддалений адміністратор реєстрації приймає та розглядає документи, надані заявником (його довіреною особою) протягом однієї години з моменту надходження заяви.

Адміністратор реєстрації АЦСК ІДД Міндоходів або віддалений адміністратор реєстрації приймає рішення про відмову в реєстрації за результатом розгляду поданих документів у разі:

- відсутності всіх необхідних для реєстрації документів;
- відсутності у довіреної особи документів, які засвідчують її повноваження та особу;
- поданні заявником неналежно засвідчених копій документів;
- невідповідності даних, що визначені в поданих документах, фактичним даним заявника.

У випадку відмови в реєстрації заява на реєстрацію разом з додатками повертається заявнику з позначкою адміністратора реєстрації або віддаленого адміністратора реєстрації про відмову із зазначенням підстав.

При ухваленні позитивного рішення адміністратор реєстрації АЦСК ІДД Міндоходів або віддалений адміністратор реєстрації виконує реєстраційні дії по занесенню реєстраційної інформації до реєстру абонентів АЦСК ІДД Міндоходів.

Реєстрація заявника є підставою для генерації ключів та формування посиленого сертифікату ключа підписувача.

5.5. Порядок повторної реєстрації заявника після закінчення строку обслуговування посиленого сертифікату ключа

Процедура повторної реєстрації заявника після закінчення строку обслуговування посиленого сертифікату ключа здійснюється у відповідності до первинної процедури реєстрації заявника, за винятком того, що при повторній реєстрації не формується нова особова справа заявника, а здійснюється актуалізація документів у існуючій особовій справі та реєстраційних даних в реєстрі підписувачів АЦСК ІДД Міндоходів на підставі поданої заявником інформації.

5.6. Внесення змін до реєстраційних даних заявника (підписувача) або позапланова заміна посиленних сертифікатів ключів

У разі зміни даних заявника (підписувача) заявник зобов'язується невідкладно заблокувати сертифікати ключів підписувачів данні яких змінилися та подати до АЦСК ІДД Міндоходів або

відокремлених пунктів реєстрації АЦСК ІДД Міндоходів заяву відповідного зразка та документи, що підтверджують достовірність зміни реєстраційних даних.

У разі необхідності позапланової заміни посиленних сертифікатів ключів підписувачів заявник подає до АЦСК ІДД Міндоходів або відокремлених пунктів реєстрації АЦСК ІДД Міндоходів заяву відповідного зразка та документи необхідні формування нових сертифікатів підписувачів.

На підставі звернення та наданих документів адміністратор реєстрації АЦСК ІДД Міндоходів або відділений адміністратор реєстрації здійснює ідентифікацію (встановлення) особи заявника та перевірку наданих документів (відомостей).

5.7. Автентифікація підписувача під час звернення щодо блокування, скасування та поновлення посиленого сертифіката ключа

В залежності від порядку звернення щодо блокування, скасування та поновлення посиленого сертифіката ключа передбачені різні форми автентифікації підписувача та перевірки законності такого звернення:

- у разі письмового звернення підписувача, законність звернення встановлюється за власноручним підписом та печаткою юридичної особи (для юридичних осіб);
- у разі звернення шляхом направлення запиту на блокування або скасування посиленого сертифіката в електронному вигляді, законність звернення встановлюється шляхом перевірки ЕЦП на запиті за допомогою чинного посиленого сертифіката підписувача;
- у разі звернення щодо блокування посиленого сертифіката ключа по телефону, законність звернення встановлюється за паролем фразою, що вказується підписувачем під час реєстрації.

5.8. Захист персональних даних підписувачів забезпечується шляхом вжиття:

- організаційних заходів щодо обліку та зберігання справ підписувачів, зокрема формування справи підписувачів та їх облік, призначення відповідальної особи за зберігання справ підписувачів, обмежений доступ обслуговуючого персоналу до приміщення (шаф), де зберігаються справи підписувачів;
- організаційно-технічних та технічних заходів реалізованих комплексною системою захисту інформації автоматизованої системи АЦСК ІДД Міндоходів (далі – КСЗІ), у тому числі: використанням надійних засобів ЕЦП, веденням журналів роботи системи у захищеному вигляді, розмежування та контролю інформаційних потоків між внутрішньою локальною мережею АЦСК ІДД Міндоходів та підсистемою відкритого доступу, використанням антивірусних засобів, міжмережевих екранів тощо.

6. Процедури та механізми обслуговування посиленних сертифікатів ключів

6.1. Порядок генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані:

- на робочому місці підписувача;
- на робочій станції генерації ключів в АЦСК ІДД Міндоходів.

Для генерації відкритого та особистого ключів на робочому місці підписувача застосовуються надійні засоби ЕЦП. При цьому генерація здійснюється з використанням технічних засобів заявника. Згенерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе підписувач.

Засоби генерації ключів формують запит на формування сертифіката у відповідному форматі, що містить відкритий ключ підписувача і додаткову інформацію для формування посиленого сертифіката у АЦСК ІДД Міндоходів.

Передача до АЦСК ІДД Міндоходів сформованого підписувачем запиту здійснюється на носії інформації особисто підписувачем або його довіреною особою після процедури реєстрації заявника.

У разі генерації відкритого та особистого ключа підписувача у АЦСК ІДД Міндоходів ключі генеруються ним особисто на робочій станції генерації ключів, що входить до складу програмно-технічного комплексу АЦСК ІДД Міндоходів. Особистий ключ підписувача записується на носій ключової інформації та залишається у нього, а сформований запит на формування сертифіката передається через службовий носій інформації на робочу станцію адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються в АЦСК ІДД Міндоходів. Після генерації та запису на носій ключової інформації вони знищуються надійним способом.

Строк дії особистого ключа підписувача становить не більше двох (2) років. Початком строку дії особистого ключа вважається дата та час формування сертифіката, що містить відкритий ключ відповідний до особистого.

6.2. Порядок подання запиту на сертифікацію

Для формування сертифікату ключа використовується запит на формування сертифікату ключа, який створюється в процесі генерації особистого та відкритого ключів ЕЦП. Запит на сертифікацію може подавати заявник, що пройшов процедуру реєстрації або підписувач (у разі позапланової заміни ключів).

Після генерації особистого та відкритого ключів ЕЦП, підписувач передає запит на формування сертифікату ключа адміністратору реєстрації. Якщо генерація особистого та відкритого ключів ЕЦП була проведена за межами АЦСК ІДД Міндоходів, адміністратор реєстрації проводить перевірку належності підписувачу особистого ключа ЕЦП та його відповідність відкритому ключу.

Процедура подання запиту на сертифікацію для підписувачів, які мають чинний сертифікат ключа ідентична процедурі подання запиту на сертифікацію для нового підписувача.

6.3. Порядок формування посилених сертифікатів та надання їх абонентам

Після ідентифікації та реєстрації заявника відповідно до п. 5 Регламенту та генерації ключів підписувача, адміністратор реєстрації виконує процедуру перевірки унікальності відкритого ключа підписувача в реєстрі посилених сертифікатів ключів АЦСК ІДД Міндоходів, включає дані про обмеження сфери використання ЕЦП, інші дані на вимогу заявника та надсилає електронний запит у захищеному вигляді до АЦСК ІДД Міндоходів для формування посиленого сертифіката.

Сформований посилений сертифікат ключа вноситься до реєстру сертифікатів ключів АЦСК ІДД Міндоходів на інформаційному ресурсі АЦСК ІДД Міндоходів.

Адміністратор реєстрації записує сформований посилений сертифікат ключа на електронний носій інформації заявника. Виготовлення посиленого сертифікату ключа на паперовому носії здійснюється на вимогу підписувача у двох примірниках та засвідчується власноручним підписом підписувача, адміністратора реєстрації та засвідчується печаткою АЦСК ІДД Міндоходів (відокремленого пункту реєстрації).

У випадку реєстрації заявника через відокремлений пункт реєстрації заявників копії сертифіката у паперовій формі виготовляє та підписує віддалений адміністратор реєстрації.

По завершенню процедури формування посиленого сертифікату ключа заявнику (підписувачу) надаються:

- Посилений сертифікат ключа в електронному вигляді, записаний на електронний носій інформації заявника (підписувача);
- надійні засоби ЕЦП;
- посилений сертифікат ключа в роздрукованому вигляді (на вимогу заявника).

Строк чинності посиленого сертифікату ключа не може перевищувати два (2) роки.

Після отримання посиленого сертифікату ключа підписувач повинен перевірити достовірність відомостей викладених у ньому. При виявленні недостовірних даних або помилок підписувач повинен повідомити АЦСК ІДД Міндоходів (відокремлений пункт реєстрації) в порядку визначеному для скасування сертифікату ключа. Після скасування сертифікату та виправлення реєстраційних даних формується новий посилений сертифікат ключа.

Заявник (підписувач) підтверджує факт отримання посиленого сертифікату ключа та достовірність даних викладених у ньому шляхом підписання акту виконаних робіт.

6.4. Порядок повторного формування посиленого сертифікату ключа

Повторне формування посиленого сертифікату ключа полягає у формуванні нового сертифікату ключа у разі передчасного (протягом строку обслуговування) скасування чинного сертифікату ключа через компрометацію особистого ключа або зміну відомостей про підписувача зазначених у сертифікаті ключа.

При повторному формуванні посиленого сертифіката ключа адміністратор реєстрації здійснює перевірку дійсності даних, які були надані заявником під час реєстрації.

При виникненні необхідності зміни даних, зазначених у посиленому сертифікаті ключа підписувача, АЦСК ІДД Міндоходів (відокремлений пункт реєстрації) може здійснити формування нового посиленого сертифіката ключа із використанням попередньо засвідченого відкритого ключа підписувача, у разі якщо відповідний йому особистий ключ не був скомпрометований. При цьому сумарний строк чинності особистого ключа не може перевищувати двох (2) років.

6.5. Використання посиленого сертифіката та особистого ключа

Права та обов'язки заявника

Заявник зобов'язаний:

- ознайомитись з умовами надання послуг ЕЦП, визначених цим Регламентом та відповідними нормативними документами, та дотримуватись них;
- надавати повну та дійсну інформацію під час реєстрації, необхідну для формування сертифіката ключа підписувача;
- зберігати у таємниці особистий ключ ЕЦП та вживати усіх можливих заходів для запобігання його втрати, розкриття, перекручування чи несанкціонованого використання;
- не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу голосової автентифікації;
- не розголошувати та не повідомляти іншим особам пароль доступу до захищеного носія ключової інформації, на якому знаходиться особистий ключ ЕЦП;
- використовувати особистий ключ виключно для мети, визначеної у сертифікаті, та додержуватись інших обмежень щодо сфери використання сертифіката ключа;
- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
- негайно інформувати АЦСК ІДД Міндоходів про наступні події, що трапилися до закінчення строку чинності сертифіката ключа: компрометацію особистого ключа; компрометацію паролю захисту особистого ключа; виявлені неточності або зміни даних, зазначених у сертифікаті;
- не використовувати особистий ключ у разі його компрометації;
- не використовувати особистий ключ, відповідний до сертифіката ключа, заява на скасування чи блокування якого подана до АЦСК ІДД Міндоходів, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування сертифіката ключа;
- не використовувати для накладання ЕЦП особистий ключ, відповідний до сертифіката ключа, що скасований або блокований.

Якщо заявник та підписувач є різними суб'єктами, заявник повинен зобов'язати підписувача виконувати вимоги Регламенту.

Заявник має право:

- своєчасно отримувати якісні послуги ЕЦП;
- цілодобового вільного доступу з використанням телекомунікаційних мереж загального користування до сертифікатів ключів інших підписувачів, даних про статус сертифікатів ключів, сертифіката ключа АЦСК ІДД Міндоходів, нормативних документів з питань надання послуг ЕЦП;
- одержувати сертифікати ключів АЦСК ІДД Міндоходів;
- одержувати список відкликаних сертифікатів, сформований АЦСК ІДД Міндоходів;
- застосовувати сертифікати ключів АЦСК ІДД Міндоходів для перевірки справжності ЕЦП сертифікатів ключів, сформованих АЦСК ІДД Міндоходів;
- застосовувати список відкликаних сертифікатів, сформований АЦСК ІДД Міндоходів, для перевірки статусу власного сертифіката ключа та сертифікатів ключів інших підписувачів;
- ознайомлюватись з інформацією щодо діяльності АЦСК ІДД Міндоходів та надання послуг ЕЦП;
- подавати заяви та скарги;
- вимагати скасування, блокування або поновлення свого сертифіката ключа.
- вимагати від АЦСК ІДД Міндоходів усунення порушень умов Регламенту та договору про надання послуг ЕЦП;
- вимагати від АЦСК ІДД Міндоходів виконання вимог захисту персональних даних підписувача;
- оскаржити дії чи бездіяльність АЦСК ІДД Міндоходів у судовому порядку.

Обов'язки користувача

Користувач зобов'язаний:

- використовувати надійні засоби ЕЦП;
- підтверджувати ЕЦП з використанням чинних посиленних сертифікатів ключів АЦСК ІДД Міндоходів;
- під час перевірки ЕЦП використовувати посилений сертифікат ключа, чинний на момент накладення ЕЦП.

6.6. Підстави та порядок скасування, блокування та поновлення посилених сертифікатів ключів

6.6.1. Підстави та порядок скасування посилених сертифікатів ключів підписувачів

Скасування сертифіката ключа є достроковим припиненням чинності сертифіката ключа. Скасовані сертифікати ключів поновленню не підлягають. АЦСК ІДД Міндоходів негайно скасовує сформований сертифікат ключа підписувача у разі:

- набрання законної сили рішенням суду про скасування посиленого сертифіката ключа;
- смерті підписувача або оголошення його померлим за рішенням суду;
- визнання підписувача недієздатним за рішенням суду;
- припинення діяльності суб'єкта господарювання – заявника;
- розірвання підписувачем трудового договору з юридичною особою – заявником;
- надання заявником недостовірних даних;
- не поновлення заявником заблокованого сертифіката протягом 30 календарних днів;
- припинення (розірвання) договору з заявником;
- за заявою заявника або його уповноваженого представника.

6.6.2. Обставини, за яких сертифікат повинен бути скасований заявником

Підписувач (заявник – юридична особа) зобов'язаний невідкладно звернутися до АЦСК ІДД Міндоходів за скасуванням сертифіката ключа у разі:

- компрометації особистого ключа підписувача (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа із будь-яких обставин, зокрема, втрата або пошкодження носія ключової інформації тощо);
- зміни відомостей, зазначених у сертифікаті ключа: переведення на іншу посаду або звільнення з роботи підписувача (для сертифікатів, в яких зазначено посада його власника); зміна прізвища; виявлення помилок у реквізитах сертифіката ключа тощо.

Документи, що були підставою для скасування, блокування або поновлення сертифіката ключа, фіксуються та зберігаються у АЦСК ІДД Міндоходів.

6.6.3. Порядок скасування посилених сертифікатів ключів

Для скасування сертифіката ключа заявник зобов'язаний подати до АЦСК ІДД Міндоходів або відокремленого пункту реєстрації письмову заяву встановленого зразка, засвідчену його особистим підписом. Якщо заявником є юридична особа, заява засвідчується підписом уповноваженого представника та печаткою юридичної особи.

Подача заяви на скасування сертифіката ключа здійснюється тільки протягом робочого дня АЦСК ІДД Міндоходів. У разі, неможливості подання заяви особисто підписувачем, він може надати довірчій особі повноваження для скасування його сертифіката ключа.

Обробка заяви на скасування сертифіката ключа та інформування заявника (підписувача) про скасування здійснюється протягом двох (2) годин з моменту надходження до АЦСК ІДД Міндоходів заяви на скасування сертифікату.

Часом скасування сертифіката ключа вважається час зміни його статусу в реєстрі сертифікатів АЦСК ІДД Міндоходів.

Підписувач не має права використовувати особистий ключ для накладення ЕЦП, сертифікат ключа якого скасовано.

У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення спричинення майнової шкоди, заявник (підписувач) блокує сертифікат такого особистого ключа в усній формі та протягом семи (7) днів зобов'язується подати відповідні заяви про блокування та скасування сертифіката ключа.

6.6.4. Порядок блокування посилених сертифікатів ключів

Під блокуванням сертифіката ключа розуміється тимчасове припинення чинності сертифіката ключа.

Після блокування сертифіката ключа, заявник зобов'язаний протягом 30 календарних днів поновити строк чинності сертифіката ключа або подати заяву про його скасування. У випадку, якщо

протягом зазначеного строку заявник не поновить чинності блокуваного сертифіката ключа та не подасть заяви про його скасування, по закінченню вищезазначеного строку такий сертифікат ключа автоматично скасовується АЦСК ІДД Міндоходів.

Блокування сертифіката ключа здійснюється на підставі заяви заявника (підписувача): в усній, письмовій формі, чи у вигляді електронного документа.

Часом блокування сертифіката ключа вважається час зміни його статусу у реєстрі сертифікатів АЦСК ІДД Міндоходів.

6.6.5. Блокування посиленого сертифіката за заявою в усній формі

Заява в усній формі подається заявником (підписувачем) до АЦСК ІДД Міндоходів засобами телефонного зв'язку за номером, який опублікований АЦСК ІДД Міндоходів на власному інформаційному ресурсі, при цьому заявник повинен повідомити адміністратору реєстрації наступну інформацію:

- ідентифікаційні дані власника сертифіката;
- ключову фразу голосової автентифікації;
- реєстраційний номер сертифіката ключа.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу голосової фрази та ідентифікаційних даних підписувача з інформацією в реєстрі користувачів).

Усна заява може бути подана цілодобово. Обробка усної заяви на блокування сертифіката та інформування власника сертифіката здійснюється протягом тридцяти (30) хвилин з моменту подачі заяви. Усна заява повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття усної заяви.

6.6.6. Блокування посиленого сертифіката за заявою у письмовій формі

Письмова заява подається до АЦСК ІДД Міндоходів або до відокремленого пункту реєстрації за встановленою формою та засвідчується власноручним підписом заявника (підписувача).

У разі якщо власником сертифіката є юридична особа, підпис уповноваженого представника юридичної особи засвідчується печаткою.

Подача заяви на блокування сертифіката ключа здійснюється тільки протягом робочого дня АЦСК ІДД Міндоходів. У разі, неможливості подання заяви особисто підписувачем, він може надати довірчій особі повноваження для блокування його сертифіката ключа.

Обробка такої заяви та інформування заявника про блокування повинні бути здійснені протягом двох (2) годин з моменту подачі заяви.

6.6.7. Блокування посиленого сертифіката ключа за електронним запитом

Електронний запит на блокування сертифіката ключа передається до ПТК АЦСК ІДД Міндоходів у вигляді вкладення у вигляді HTTP-запиту.

Електронний запит формується підписувачем за допомогою програмних засобів, які надаються АЦСК ІДД Міндоходів.

Електронний запит на блокування сертифіката ключа засвідчується ЕЦП відповідного сертифіката ключа підписувача.

У разі передачі запиту на блокування сертифіката ключа у вигляді HTTP-запиту, обробка запиту та інформування підписувача про блокування здійснюються в режимі реального часу.

У разі передачі запиту на блокування сертифіката ключа засобами електронної пошти, обробка запиту та інформування підписувача про блокування повинні бути здійснені протягом 2 (двох) годин після отримання запиту АЦСК ІДД Міндоходів.

Заява у вигляді електронного запиту повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття АЦСК ІДД Міндоходів електронного запиту.

6.6.8. Порядок поновлення чинності посилених сертифікатів ключів

Поновлення чинності сертифіката ключа можливе лише для заблокованих сертифікатів ключів, термін блокування яких не скінчився.

Для здійснення поновлення чинності сертифіката ключа, заявник подає до АЦСК ІДД Міндоходів або відокремленого пункту реєстрації, письмову заяву встановленого зразку.

Подача заяви на поновлення чинності сертифіката ключа здійснюється тільки протягом робочого дня АЦСК ІДД Міндоходів. У разі, неможливості подання заяви особисто підписувачем, він може надати довірчій особі повноваження для поновлення чинності його сертифіката ключа.

Обробка письмової заяви на поновлення чинності сертифіката ключа та інформування заявника про поновлення повинні бути здійснені протягом двох (2) годин з моменту подачі заяви.

Часом поновлення чинності сертифіката ключа вважається час зміни його статусу у реєстрі сертифікатів ключів АЦСК ІДД Міндоходів.

6.7. Закінчення строку чинності посиленого сертифіката ключа підписувача

Строк дії особистого та відкритого ключа дорівнює строку чинності відповідного сертифіката ключа.

Після закінчення строку чинності сертифіката ключа, він вилучається з інформаційного ресурсу АЦСК ІДД Міндоходів та переміщується до архіву.

АЦСК ІДД Міндоходів зберігає сертифікат та пов'язані з ним списки відкликаних сертифікатів безстроково. За запитом користувачів, АЦСК ІДД Міндоходів надає доступ до необхідного сертифіката та пов'язаних з ним списків відкликаних сертифікатів з архівних записів АЦСК ІДД Міндоходів.

6.8. Розповсюдження інформації про статус сертифікатів ключів

Для розповсюдження інформації про статус сертифікатів ключів підписувачів використовується механізм списку відкликаних сертифікатів та механізм визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP.

У разі скасування (блокування, поновлення) сертифіката, оновлений список відкликаних сертифікатів випускається та публікується не пізніше двох (2) годин після отримання запиту на відкликання сертифіката.

АЦСК ІДД Міндоходів надає всім користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер АЦСК ІДД Міндоходів.

Якщо запит сформовано вірно, OCSP – сервер повертає відповідь на запит з інформацією про статус сертифіката.

6.9. Порядок надання послуг визначення статусу сертифіката в інтерактивному режимі (онлайн перевірки статусу сертифікату)

Служба інтерактивного визначення статусу сертифіката (далі – OCSP сервер) – сервісна служба АЦСК ІДД Міндоходів, яка за запитами користувачів визначає статус сертифікатів та надсилає відповідь, де зазначається статус сертифіката, який перевіряється, на даний момент.

Вимоги до протоколу визначення статусу сертифіката засновані на міжнародному стандарті RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP».

Передача запиту на перевірку статусу сертифіката відбувається за допомогою методу GET або POST протоколу HTTP. Для передачі запиту на формування статусу сертифіката та отримання відповіді застосовується транспортний протокол HTTP.

Звичайно стан чинності сертифікату визначається за присутністю запиту про запрошувальний сертифікат у списках CRL, які формуються із заданою періодичністю. Служба OCSP дозволяє отримати інформацію про стан сертифікату безпосередньо у будь-який момент часу, навіть якщо запису про зміну стану сертифікату в CRL списках ще немає.

Запит на інтерактивну перевірку статусу сертифіката виконується ПЗ підписувача АЦСК ІДД Міндоходів за протоколом OCSP, та представляється у вигляді повідомлення «OCSPRequest». Відповідь на інтерактивну перевірку статусу сертифіката надається у вигляді повідомлення «OCSPResponse». Формування та додержання вимог протоколу та аналіз одержаного відгуку цілком покладається на програмне забезпечення підписувача (надійні засоби ЕЦП).

Служба OCSP надає послуги в режимі транзакції, тобто кожному запиту відповідає один і лише один відгук, ініціатором транзакції виступає підписувач (програмне забезпечення підписувача). Транзакція служби OCSP починається з підготовки запиту у визначеному форматі клієнтським програмним забезпеченням, яке надсилає його до служби OCSP.

Якщо відповідь отримана від OCSP – сервера відповідає п. 2.14 вимог до протоколу визначення статусу сертифіката, затвердженого наказом Міністерства юстиції України, Адміністрації державної служби спеціального зв'язку та захисту інформації від 20.08.2012 №1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису» (із змінами), а OCSPResponseStatus дорівнює нулю, результат отриманого стану чинності сертифіката вважається достовірним і може бути використаний в подальшій роботі.