НОМЕР НА ДОСИЕТО: 2022-0941
ИДЕНТИФИКАЦИОНЕН НОМЕР НА КЛАСИФИКАЦИЯТА: 3.2.3

Рамка за доверие

за електронната идентификация в Швеция

Версия от 04.10.2022 г.

1. Контекст и цел

С рамката за доверие за електронна идентификация в Швеция се цели да се установят общи изисквания за издателите на документи за електронна самоличност, разгледани и одобрени от Шведската агенция за цифрово управление (DIGG). Изискванията са разделени на различни нива на защита — известни като нива на осигуреност — които съответстват на различни степени на техническа и оперативна сигурност от страна на издателя и различни степени на проверка, че лицето, на което се издава документ за електронна идентификация, действително е лицето, за което се представя.

Изискванията на тази рамка за доверие се прилагат за нива на осигуреност 2—4, като ниво 4 съответства на най-високото ниво на защита.

Съответствието се тълкува по следния начин:

(a) когато нивото на осигуреност не е определено, изискването следва да бъде изпълнено на всички нива, и

(b) когато нивото на осигуреност е определено, съответствието следва да бъде гарантирано най-малко на съответното ниво.

Изискванията, определени за по-ниско ниво от съответното, се пренебрегват.

2. Организация и управление

Общи оперативни изисквания

K2.1 Издателите на електронна идентификация в Швеция, които не са публични органи, следва да извършват дейност в качеството на регистрирани юридически лица и да сключват и поддържат застраховката, необходима за стопанската дейност.

K2.2 Издателите на електронна идентификация в Швеция трябва да имат установена стопанска дейност, да функционират пълноценно във всички части, посочени в настоящия документ, и да са добре запознати с правните изисквания, които са им наложени в качеството на издатели на електронна идентификация в Швеция.

K2.3 Издателите на електронна идентификация в Швеция трябва да бъдат в състояние да поемат риска от отговорност за вреди и да разполагат с достатъчно финансови ресурси, за да извършват своите дейности в продължение на най-малко една година.

Сигурност на информацията

K2.4 Издателите на електронна идентификация в Швеция следва да са установили система за управление на сигурността на информацията (ИУСИ) за частите от своите дейности, засегнати от рамката за доверие, която се основава, когато е приложимо, на ISO/IEC 27001 или еквивалентни принципи за управлението и контрола на работата по сигурността на информацията, включително следното:

(a) Всички административни и технически процеси от критично значение за безопасността трябва да бъдат документирани и да се основават на формална основа, при която ролите, отговорностите и правомощията са ясно определени.

(b) Издателите на електронна идентификация в Швеция следва да гарантират, че те разполагат по всяко време с достатъчно човешки ресурси, за да изпълняват своите задължения.

(c) Издателите на електронна идентификация в Швеция установяват процес за управление на риска, с който, по подходящ начин, непрекъснато или най-малко веднъж на всеки 12 месеца се анализират заплахите и уязвимостите в стопанската дейност и, с който, чрез въвеждането на мерки за сигурност, се балансират рисковете до приемливи нива.

(d) Издателите на електронна идентификация в Швеция установяват процес за управление на инцидентите, с който систематично се гарантира качеството на услугата, формите на последващо докладване и, с който се предприемат подходящи ответни и превантивни мерки за смекчаване или предотвратяване на вреди, произтичащи от такива събития.

(e) Издателите на електронна идентификация в Швеция изготвят и редовно изпитват план за непрекъснатост, който отговаря на изискванията за достъпност на стопанската дейност, чрез способност за възстановяване на процеси от критично значение в случай на криза или сериозни инциденти.

(f) Издателите на електронна идентификация в Швеция редовно оценяват работата по сигурността на информацията и въвеждат мерки за подобряване в системата за управление.

K2.5 Обхват и зрелост на системата за управление:

Ниво 4: Системата за управление на сигурността на информацията следва да бъде в съответствие със SS-ISO/IEC 27001:2017 или еквивалентни последващи или международни версии на стандарта, както и в обхвата на настоящото да се включват всички изисквания, наложени на издателите на електронна идентификация в Швеция.

Условия за възлагане на дейности на подизпълнители

K2.6 Даден издател на електронна идентификация в Швеция, който е възложил изпълнението на един или повече процеси от критично значение за сигурността на друга страна, следва да определи чрез договор кои процеси от критично значение са отговорност на подизпълнителя и кои изисквания са приложими за тях, както и да разясни договорните отношения в декларацията на издателя.

Проследимост, заличаване и съхранение на документи

K2.7 Издателите на електронна идентификация в Швеция следва да съхраняват:

(a) документи за подаване на заявления и документи, свързани с издаването, получаването или блокирането на електронна идентификация;

(b) договори, документи за политики и декларации на издателя; и

(c) история на обработката и друга такава документация, тъй като се изисква доказване на спазването на изискванията, наложени на издателите на електронна идентификация в Швеция, и с която се предоставя възможност за последващи действия, с които се доказва, че процесите и проверките от критично значение за сигурността са въведени и ефективни.

K2.8 Периодът на съхранение не може да бъде по-кратък от пет години и материалът следва да може да се произвежда в четлива форма през целия този период, освен ако изискване за заличаване не е необходимо от гледна точка на неприкосновеността на личния живот и е подкрепено със закон или друга наредба.

Преглед и последващи действия

K2.9 Издателите на електронна идентификация в Швеция следва да установят функция за вътрешен одит, с която периодично да се преглеждат дейностите по издаване. Вътрешният одитор следва да бъде независим при изпълнението на своите задължения по начин, с който се гарантира обективен и безпристрастен преглед, както и да притежава компетентността и експертния опит, необходими за изпълнението на неговите или нейните задължения. Вътрешният одитор следва независимо да планира провеждането на одита и да го документира в план за одит, обхващащ период от три години. Елементите на одита следва да се подбират въз основа на анализ на риска и съществеността и да се основават на описанията на дейностите, представени от издателя пред Агенцията за цифрово управление.

Нива 3 и 4: Вътрешният одит следва да се извършва въз основа на приетите стандарти за одит.

3. Физическа, административна и ориентирана към личността сигурност

K3.1 Централните части на дейността следва да бъдат физически защитени срещу вреди в резултат на екологични събития, неразрешен достъп или други външни смущения. Контролът на достъпа следва да се прилага по такъв начин, че достъпът до чувствителни зони да бъде ограничен до упълномощения персонал, носителите на информация да се съхраняват и обезвреждат по сигурен начин, а достъпът до тези защитени зони да се наблюдава непрекъснато.

K3.2 Преди дадено лице да поеме някоя от ролите, определени в съответствие с K2.4, буква а), и които са от особено значение за сигурността, издателят на електронна идентификация в Швеция следва да е извършил цялостни проверки, за да се гарантира, че лицето може да бъде считано за надеждно и че лицето притежава квалификациите и обучението, изисквани за безопасното и сигурното изпълнение на задачите, произтичащи от ролята.

K3.3 Издателите следва да са въвели процедури, за да се гарантира, че само специално упълномощени служители имат достъп до данните, събрани и запазени в съответствие с K2.7.

K3.4 **Нива 3 и 4:** Издателите гарантират по цялата верига на процеса на издаване, че разделението на задълженията се прилага по такъв начин, че нито едно лице да не може да получи електронна идентификация от името на друго лице.

4. Техническа сигурност

K4.1 Издателите на електронна идентификация в Швеция следва да гарантират, че въведеният технически контрол е достатъчен, за да се постигне нивото на защита, считано за необходимо с оглед на естеството, обхвата и други обстоятелства, свързани със стопанската дейност, и че този контрол функционира и е ефективен.

K4.2 Електронните средства за комуникация, използвани при предаването на чувствителни данни, са защитени срещу прихващане, манипулиране и повторно възпроизвеждане.

K4.3 Чувствителните криптографски материали, служещи за заключване/отключване на информацията, използвани за издаване на електронна идентификация, идентифициране на притежателите и издаване на удостоверения за самоличност, следва да бъдат защитени по такъв начин, че:

(a) достъпът да бъде ограничен, логически и физически, до ролите и приложенията, които са строго необходими;

(b) материалите, служещи за заключване/отключване на информацията, никога не следва да се съхраняват в обикновен текст върху постоянни носители за съхранение;

(c) материалите, служещи за заключване/отключване на информацията, да бъдат защитени чрез използването на криптографски хардуерен модул с активни механизми за сигурност, с които да се противодейства както на физически, така и на логически опити за компрометиране на материалите, служещи за заключване/отключване на информацията;

(d) механизмите за сигурност за защитата на материалите, служещи за заключване/отключване на информацията, да бъдат прозрачни и да бъдат основавани на признати и утвърдени стандарти; и

(e) **Нива 3 и 4:** данните за активиране за защита на материалите, служещи за заключване/отключване на информацията, да бъдат управлявани чрез контрол от няколко лица.

K4.4 Издателите следва да са въвели документирани процедури, за да се гарантира, че изискваното ниво на защита в съответната информационна среда може да бъде поддържано с течение на времето и във връзка с промените, включително редовни оценки на уязвимостта, както и подходяща готовност за посрещане на променящите се нива на риск и инцидентите, които възникват.

5. Подаване на заявление, идентифициране и регистрация

Информация относно условията

K5.1 Издателите на електронна идентификация в Швеция предоставят информация за договорите, общите условия, както и свързаната информация и всички ограничения относно използването на услугата, на свързаните потребители, доставчиците на електронни услуги и други лица, които могат да разчитат на услугата на издателя.

K5.2 Даден издател на електронна идентификация в Швеция следва ясно да посочи общите условия и да определи процедурите, така че общите условия да бъдат предоставени на заявителя в хода на процеса на издаване.

K5.3 Издателите на електронна идентификация в Швеция предоставят декларация на издателя, която включва:

(a) самоличността и данните за контакт на издателя;

(b) кратки описания на услугите и решенията, предоставяни от издателя, включително прилаганите методи за подаване на заявление, издаване и блокиране;

(c) условията, свързани с предоставяната услуга, включително задълженията на ползвателя за защита на неговата електронна идентификация, задълженията и отговорностите на издателя, всички предоставени гаранции и обещаната наличност;

(d) информация относно обработването на лични данни и начина, по който то се извършва; и

(e) договорености за изменение на общите условия или другите условия на предоставяната услуга, включително стъпките, които следва да бъдат предприети за прекратяване на услугата по контролиран начин.

K5.4 **Нива 3 и 4:** По искане на Агенцията за цифрово управление (DIGG) или друга договаряща страна, която разчита на услугите, предоставяни от издателя, издателите на електронна идентификация в Швеция предоставят информация относно това как се притежава и управлява стопанската дейност.

K5.5 Даден издател на електронна идентификация в Швеция, който прекратява своята дейност, следва предварително изготвен план за прекратяване на услугата. Планът следва да включва информиране на всички ползватели на услугата и DIGG. Освен това издателят следва да съхранява архивираните материали на разположение в съответствие с K2.7 и K2.8 след прекратяването.

Подаване на заявление

K5.6 Електронната идентификация в Швеция може да бъде издадена само по искане на заявителя или чрез друга еквивалентна процедура за приемане и само след като заявителят е бил уведомен за условията, при които тя се издава, както и за отговорността, която ще бъде възложена на него или нея.

Издаването на електронна идентификация обаче, която заменя или допълва валиден или наскоро блокиран документ за електронна идентификация, издаден преди това от същия издател, може да се извърши без предварителна процедура за подаване на заявление.

K5.7 Дадено заявление за електронна идентификация в Швеция следва да бъде свързано с личен идентификационен номер или координационен номер, както и с информацията, която е необходима за издателя, за да предостави такава електронна идентификация.

Определяне на самоличността на заявителя

K5.8 Издателите на електронна идентификация в Швеция трябва да проверят дали информацията, свързана със заявлението, е пълна и съответства на информацията, регистрирана в официален регистър.

K5.9 Когато информацията, която следва да бъде проверена в официален регистър, е обозначена като поверителна („защитена самоличност“), необходимите проверки могат да бъдат извършени чрез други еквивалентни средства.

K5.10 Идентифициране на заявителя по време на присъствено посещение:

издателите на електронна идентификация в Швеция могат да проверят самоличността на заявителя по време на присъствено посещение по същия начин, както при издаването на стандартен документ за самоличност.

K5.11 Идентифициране от разстояние на заявителяпри съществуващоотношение:

Ниво 3: Издателите на електронна идентификация в Швеция, които вече са идентифицирали заявителя при отношения, включващи значими трансакции в икономическо или правно отношение, и при които заявителят може да бъде идентифициран от разстояние чрез други надеждни средства, еквивалентни на изискванията за ниво 3 на знака за качество на електронната идентификация в Швеция, могат да използват този метод, за да установят самоличността на заявителя.

Ниво 4: Не е приложимо.

K5.12 Идентифициране чрез електронна идентификация в Швеция:

Даден издател на електронна идентификация в Швеция може да идентифицира заявителя от разстояние чрез съществуваща валидна електронна идентификация в Швеция с най-малко същото ниво на осигуреност като тази, която следва да бъде издадена, ако може, без договорни пречки, да използва такава идентификация като основание за издаване на нова електронна идентификация.

Ниво 4: Срокът на валидност на новоиздадената електронна идентификация следва да бъде ограничен до срока на валидност на съществуващата електронна идентификация.

K5.13 Идентифициране от разстояние на заявителя:

Ниво 2: Издателите на електронна идентификация в Швеция могат да използват надеждни записи на изображения на валиден стандартен документ за самоличност и портретно изображение на заявителя като основание за установяване от разстояние на самоличността на заявителя, ако сравнението не поражда съмнения относно неговата истинска самоличност.

Ниво 3: Издателите на електронна идентификация в Швеция могат, чрез обезопасено четене на валиден стандартен документ за самоличност, съдържащ съхранявани в електронен формат биометрични данни, да установят самоличността на заявителя от разстояние въз основа на тези данни, ако съответните биометрични данни на лицето, което следва да бъде идентифицирано, могат да бъдат събрани по достатъчно обезопасен начин, така че сравнението да може да се извърши с еквивалентна надеждност, както при присъствено посещение, и когато сравнението не поражда съмнения относно истинската самоличност на заявителя.

Ниво 4: Не е приложимо.

Регистрация

K5.14 Издателите на електронна идентификация в Швеция, като вземат предвид приложимите правила за защита на личните данни, следва да поддържат регистър на свързаните ползватели и предоставените документи за електронна идентификация, както и да актуализират този регистър.

6. Издаване и блокиране на електронна идентификация

Проектиране на технически средства

K6.1 Технически средства:

Нива 2 и 3: Техническите средства за електронна идентификация чрез електронна идентификация със знак за качество на електронната идентификация в Швеция се проектират в съответствие с двуфакторен принцип, при който едната част се състои от съхранявана в електронен формат информация, която ползвателят следва да притежава, а другата се състои от това, което ползвателят следва да използва за активиране на електронната идентификация.

Ниво 4: Техническите средства за електронна идентификация чрез електронна идентификация със знак за качество на електронната идентификация в Швеция се проектират в съответствие с двуфакторен принцип, при който едната част се състои от модул за лична сигурност, който ползвателят следва да притежава, а другата се състои от това, което ползвателят следва да използва за активиране на модула за сигурност.

K6.2 Механизмът за активиране и персонализираният код се проектират по такъв начин, че да бъде малко вероятно трети страни да нарушат защитата, дори чрез механични средства.

Нива 3 и 4: Защитата включва механизми за предотвратяване на копирането и манипулирането на документа за електронна идентификация.

K6.3 Ползвателите на електронна идентификация със знак за качество на електронната идентификация в Швеция могат, по своя собствена инициатива, в рамките на срока на валидност на електронната идентификация, безплатно и без значителни неудобства, да обменят или да поискат нов личен код и, чрез насоки или автоматично производство, да бъдат подпомогнати да изпълняват изискванията на K6.2.

Ако електронната идентификация е проектирана по такъв начин, че даден персонализиран код да не може да бъде обменен, ползвателят следва вместо това, при същите условия, да може същевременно да получи нова електронна идентификация с нов персонализиран код, който заменя предишният чрез процедура на блокиране.

K6.4 Издателите на електронна идентификация в Швеция следва да гарантират, че данните, регистрирани за електронна идентификация на притежателите, еднозначно представляват заявителя и са присъщи за въпросното лице при издаването на документа за електронна идентификация.

K6.5 Срокът на валидност на издадената електронна идентификация е ограничен, като се вземат предвид характеристиките във връзка със сигурността на документа за електронна идентификация и рисковете от злоупотреба. Максималният срок на валидност на електронната идентификация е пет години.

Предоставяне на документ за електронна идентификация

K6.6 предоставяне от разстояние::

Ниво 2: Издателят на електронна идентификация в Швеция следва да предостави - документ за електронна идентификация по начин, с който се потвърждават данните за контакт, съхранявани в официалния регистър, или такава информация, вписана във връзка с електронната процедура съгласно K5.13, ниво 2.

Ниво 3: Даден издател на електронна идентификация в Швеция, който предоставя електронна идентификация чрез електронна процедура, която е в съответствие с K5.11, ниво 3, K5.12, ниво 3 или K5.13, ниво 3, когато е новоиздадена, отделно и независимо от разпоредбата по отношение на сигурността, гарантира, че ползвателят е информиран, че такъв -документ за електронна идентификация е предаден, или чрез други мерки гарантира еквивалентна степен на контрол, че лицето е предупредено за риска от кражба на самоличността във връзка с предоставянето.

Ниво 4: Даден издател на електронна идентификация в Швеция, който предоставя електронна идентификация чрез електронна процедура, съответстваща на K5.12, ниво 4, следва, когато е новоиздадена, отделно и независимо от разпоредбата по отношение на сигурността, да гарантира, че ползвателят е информиран, че такъв документ за електронна идентификация е предаден.

K6.7 Предоставяне по време на присъствено посещение:

Даден издател на електронна идентификация в Швеция, по време на присъствено посещение и след проверка на самоличността в съответствие с K5.10, следва да предостави документа за електронна идентификация срещу подписана разписка и да предостави допълнително частта, която ползвателят използва за активиране на електронната идентификация отделно и независимо от предоставянето на документа за електронна идентификация по отношение на сигурността, въз основа на данните за контакт, съхранявани в официален регистър, или друга еквивалентна информация.

Услуга за блокиране

K6.8 Издателите на електронна идентификация в Швеция следва да предоставят услуга за блокиране с добра достъпност, за да може ползвателят да блокира своята електронна идентификация.

K6.9 Издателите на електронна идентификация в Швеция своевременно и по сигурен начин следва да обработват и изпълняват исканията за блокиране и предприемат мерки за предотвратяване на системна злоупотреба с услугата за блокиране или други умишлени действия, които водят до широко разпространено блокиране на документите за електронна идентификация, като същевременно гарантират, че документите за електронна идентификация на ползвателите са на разположение, когато е необходимо.

7. Проверка на електронните самоличности на притежателите

K7.1 Издателите на електронна идентификация в Швеция следва да гарантират, че при проверката на самоличността на притежателя се извършват надеждни проверки относно автентичността и валидността на документа за електронна идентификация.

K7.2 Издателите на електронна идентификация в Швеция следва да гарантират, че при проверката на електронните самоличности на притежателите са въведени технически проверки, свързани със сигурността, така че да бъде малко вероятно трети страни, чрез предположения, подслушване, повторно възпроизвеждане или манипулиране на процеса, да могат да нарушат механизмите за защита.

8. Издаване на удостоверения за самоличност

Издателите на електронна идентификация в Швеция, които предоставят услуга за издаване на удостоверения за самоличност на доверяващи се електронни услуги, следва също така да спазват разпоредбите на настоящия член.

K8.1 Издателите на електронна идентификация в Швеция следва да гарантират, че услугата за издаване на удостоверения за самоличност има добра достъпност и че издаването на удостоверения за самоличност се предхожда от надеждна идентификация в съответствие с разпоредбите на член 7.

Ниво 4: Удостоверенията включват позоваване на криптографски материали, служещи за заключване/отключване на информацията, проверени от издателя като притежавани единствено от притежателя.

K8.2 Представените удостоверения за самоличност следва да бъдат валидни само толкова дълго, колкото е необходимо, за да се предостави на ползвателя достъп до поисканата -електронна услуга, както и да бъдат защитени така, че информацията да може да бъде прочетена само от целевия получател и автентичността на удостоверенията да може да бъде проверена от получателите на удостоверенията.

K8.3 Издателите на електронна идентификация в Швеция, като вземат предвид рисковете от злоупотреба с удостоверителната услуга, ограничават срока, в рамките на който на даден притежател могат да бъдат издадени няколко последователни удостоверения за самоличност, преди притежателят да бъде повторно идентифициран в съответствие с разпоредбите на член 7.