DOSSIERNUMMER: 2022-0941
CLASSIFICATIE-ID: 3.2.3

Het vertrouwenskader

voor Zweedse e-identificatie

Versie 4 oktober 2022

1. Achtergrond en doel

Het Vertrouwenskader voor Zweedse e-identificatie heeft tot doel gemeenschappelijke vereisten vast te stellen voor uitgevers van elektronische ID's die worden beoordeeld en goedgekeurd door het Zweedse Agentschap voor Digitale Overheid (DIGG). De vereisten zijn onderverdeeld in verschillende klassen van bescherming – zekerheidsniveaus – die overeenkomen met verschillende graden van technische en operationele veiligheid van de uitgevende instantie en verschillende graden van verificatie dat de persoon aan wie een elektronisch identificatiedocument wordt afgegeven inderdaad is wie hij of zij beweert te zijn.

De vereisten van dit vertrouwenskader zijn van toepassing op zekerheidsniveaus 2 tot en met 4, waarbij niveau 4 overeenkomt met het hoogste beschermingsniveau.

Naleving wordt als volgt geïnterpreteerd:

(a) indien het zekerheidsniveau niet is gespecificeerd, wordt op alle niveaus aan de vereiste voldaan, en

(b) indien het zekerheidsniveau wordt gespecificeerd, wordt de naleving ten minste op het relevante niveau gewaarborgd.

Vereisten die voor een lager niveau zijn vastgesteld dan het relevante niveau, worden buiten beschouwing gelaten.

2. Organisatie en governance

Algemene operationele vereisten

K2.1 Uitgevers van Zweedse eID's die geen overheidsinstanties zijn, dienen te werken als geregistreerde rechtspersonen en de voor de onderneming vereiste verzekeringen af te sluiten en te onderhouden.

K2.2 Uitgevers van Zweedse eID's dienen een gevestigd bedrijf te hebben, volledig operationeel te zijn in alle in dit document gespecificeerde delen en goed thuis te zijn in de wettelijke vereisten die aan hen worden gesteld als uitgever van Zweedse eID's.

K2.3 Uitgevers van Zweedse eID's dienen in staat te zijn het risico van aansprakelijkheid voor schade te dragen en dienen over voldoende financiële middelen te beschikken om hun activiteiten gedurende ten minste één jaar uit te voeren.

Informatiebeveiliging

K2.4 Uitgevers van Zweedse eID's hebben een beheersysteem voor informatiebeveiliging (ISMS) opgezet voor de delen van hun activiteiten die onder het vertrouwenskader vallen, dat, indien van toepassing, is gebaseerd op ISO/IEC 27001 of gelijkwaardige beginselen voor het beheer en de controle van informatiebeveiligingswerkzaamheden, met inbegrip van het volgende:

(a) Alle veiligheidskritieke administratieve en technische processen dienen te worden gedocumenteerd en te zijn gebaseerd op een formele basis, waarbij rollen, verantwoordelijkheden en bevoegdheden duidelijk zijn gedefinieerd.

(b) Uitgevers van Zweedse eID's zorgen ervoor dat zij te allen tijde over voldoende personele middelen beschikken om aan hun verplichtingen te voldoen.

(c) Uitgevers van Zweedse eID's zetten een risicobeheerproces op dat, op passende wijze, voortdurend of ten minste om de twaalf maanden, bedreigingen en kwetsbaarheden in het bedrijf analyseert en dat, door de invoering van beveiligingsmaatregelen, de risico's in evenwicht brengt tot een aanvaardbaar niveau.

(d) Uitgevers van Zweedse eID's dienen een incidentbeheerproces op te zetten dat systematisch de kwaliteit van de dienst waarborgt, vormen van verdere melding vaststelt, en ervoor zorgt dat er passende reactieve en preventieve maatregelen worden genomen om schade als gevolg van dergelijke gebeurtenissen te beperken of te voorkomen.

(e) Uitgevers van Zweedse eID's vestigen en testen een continuïteitsplan, dat voldoet aan de toegankelijkheidsvereisten van het bedrijf door kritieke processen te kunnen herstellen in geval van een crisis of ernstige incidenten.

(f) Uitgevers van Zweedse eID's evalueren regelmatig de werkzaamheden op het gebied van informatiebeveiliging en voeren verbeteringsmaatregelen in het beheersysteem in.

K2.5 Reikwijdte en rijpheid van het beheersysteem:

Niveau 4 Het beheersysteem voor informatiebeveiliging voldoet aan SS-ISO/IEC 27001:2017 of gelijkwaardige latere of internationale versies van de norm, en omvat binnen het toepassingsgebied hiervan alle vereisten die aan uitgevers van Zweedse eID's worden opgelegd.

Uitbestedingsvoorwaarden

K2.6 Een uitgever van Zweedse eID's die de uitvoering van een of meer beveiligingskritieke processen aan een andere partij heeft uitbesteed, bepaalt contractueel voor welke kritieke processen de onderaannemer verantwoordelijk is en welke vereisten daarop van toepassing zijn, en verduidelijkt de contractuele relatie in de uitgeversverklaring.

Traceerbaarheid, verwijdering en opslag van documenten

K2.7 Uitgevers van Zweedse eID's dienen het volgende op te slaan:

(a) aanvraagdocumenten en documenten met betrekking tot de afgifte, ontvangst of blokkering van eID's;

(b) contracten, beleidsdocumenten en verklaringen van de uitgevende instelling; en

(c) de verwerkingsgeschiedenis en andere documentatie die nodig is om de naleving van de aan Uitgevers van Zweedse eID's opgelegde vereisten aan te tonen en die follow-up mogelijk maakt die aantoont dat de beveiligingskritieke processen en controles aanwezig en effectief zijn.

K2.8 De opslagperiode mag niet korter zijn dan vijf jaar en het materiaal dient gedurende deze periode in leesbare vorm te kunnen worden geproduceerd, tenzij een vereiste voor verwijdering uit het oogpunt van de persoonlijke levenssfeer noodzakelijk is en wordt ondersteund door wet- of andere regelgeving.

Evaluatie en follow-up

K2.9 Uitgevers van Zweedse eID's stellen een interne auditfunctie in die de uitgifteactiviteiten periodiek evalueert. De interne auditor is onafhankelijk bij de uitvoering van zijn of haar taken op een wijze die een objectieve en onpartijdige toetsing waarborgt en beschikt over de bekwaamheid en ervaring die vereist zijn voor de uitvoering van zijn of haar taken. De interne auditor plant onafhankelijk de uitvoering van de audit en documenteert deze in een auditplan dat een periode van drie jaar bestrijkt. Auditelementen worden geselecteerd op basis van een risico- en materialiteitsanalyse en zijn gebaseerd op de beschrijvingen van verrichtingen die door de uitgever bij het Agentschap voor Digitale Overheid zijn ingediend.

Niveaus 3 en 4: De interne audit wordt uitgevoerd op basis van aanvaarde auditnormen.

3. - fysieke, administratieve en persoonsgerichte beveiliging,

K3.1 De centrale delen van de exploitatie worden fysiek beschermd tegen schade als gevolg van milieugebeurtenissen, ongeoorloofde toegang of andere externe verstoringen. De toegangscontrole wordt zodanig toegepast dat de toegang tot gevoelige gebieden wordt beperkt tot bevoegd personeel, dat informatiedragers veilig worden opgeslagen en verwijderd, en dat de toegang tot deze beschermde gebieden voortdurend wordt gecontroleerd.

K3.2 Voordat een persoon een van de overeenkomstig K2.4, onder a), geïdentificeerde rollen die van bijzonder belang zijn voor de veiligheid op zich neemt, dient de Uitgever van Zweedse eID's antecedentenonderzoeken te hebben uitgevoerd om ervoor te zorgen dat de persoon als betrouwbaar kan worden beschouwd en dat de persoon over de vereiste kwalificaties en opleiding beschikt om de uit de rol voortvloeiende taken veilig en betrouwbaar uit te voeren.

K3.3 Uitgevende instellingen dienen over procedures te beschikken om ervoor te zorgen dat alleen specifiek bevoegd personeel toegang heeft tot de overeenkomstig K2.7 verzamelde en bewaarde gegevens.

K3.4 **Niveaus 3 en 4:** Uitgevende instellingen zorgen er gedurende de hele keten van het afgifteproces voor dat de scheiding van taken zodanig wordt toegepast dat geen enkele persoon in staat is een eID op naam van een andere persoon te verkrijgen.

4. Technische beveiliging

K4.1 Uitgevers van Zweedse eID's zorgen ervoor dat de bestaande technische controles toereikend zijn om het beschermingsniveau te bereiken dat noodzakelijk wordt geacht met betrekking tot de aard, de reikwijdte en andere omstandigheden van de onderneming, en dat deze controles goed functioneren en doeltreffend zijn.

K4.2 Elektronische communicatiemiddelen die bij de doorgifte van gevoelige gegevens worden gebruikt, dienen te worden beschermd tegen onderschepping, manipulatie en herhaling.

K4.3 Gevoelig cryptografisch sleutelmateriaal dat wordt gebruikt voor de afgifte van eID's, de identificatie van houders en de afgifte van identiteitscertificaten, wordt zodanig beschermd dat:

(a) de toegang, logisch en fysiek, wordt beperkt tot de rollen en toepassingen die strikt noodzakelijk zijn;

(b) het sleutelmateriaal nooit in platte tekst wordt opgeslagen op vasthoudende opslagmedia;

(c) het sleutelmateriaal wordt beschermd door het gebruik van een cryptografische hardwaremodule met actieve beveiligingsmechanismen die zowel fysieke als logische pogingen om het sleutelmateriaal in gevaar te brengen, tegengaan;

(d) beveiligingsmechanismen voor de bescherming van sleutelmateriaal transparant zijn en worden gebaseerd op erkende en goed gevestigde normen; en

(e) **Niveaus 3 en 4:** activeringsgegevens voor de bescherming van het sleutelmateriaal worden beheerd via controle door meerdere personen.

K4.4 Uitgevers beschikken over gedocumenteerde procedures om ervoor te zorgen dat het vereiste beschermingsniveau in de relevante IT-omgeving in de loop van de tijd en in verband met wijzigingen kan worden gehandhaafd, met inbegrip van regelmatige kwetsbaarheidsbeoordelingen en passende paraatheid om te voldoen aan veranderende risiconiveaus en incidenten die zich voordoen.

5. Aanvraag, identificatie en registratie

Informatie over voorwaarden

K5.1 Uitgevers van Zweedse eID's verstrekken informatie over contracten, algemene voorwaarden, alsmede daarmee verband houdende informatie en eventuele beperkingen op het gebruik van de dienst, aan verbonden gebruikers, aanbieders van e-diensten en anderen die een beroep kunnen doen op de dienst van de uitgevende instelling.

K5.2 Een uitgever van Zweedse eID's verwijst duidelijk naar de algemene voorwaarden en ontwerpt de procedures zodanig dat de algemene voorwaarden tijdens het afgifteproces aan de aanvrager worden verstrekt.

K5.3 Uitgevers van Zweedse eID's verstrekken een uitgeversverklaring die het volgende omvat:

(a) de identiteit en contactgegevens van de uitgevende instelling;

(b) beknopte beschrijvingen van de door de uitgevende instelling aangeboden diensten en oplossingen, met inbegrip van toegepaste methoden voor toepassing, uitgifte en blokkering;

(c) voorwaarden in verband met de verleende dienst, met inbegrip van de verplichtingen van de gebruiker om zijn elektronische ID te beschermen, de verplichtingen en verantwoordelijkheden van de uitgever, eventuele garanties en beloofde beschikbaarheid;

(d) informatie over de verwerking van persoonsgegevens en de wijze waarop deze wordt uitgevoerd; en

(e) regelingen voor de wijziging van de voorwaarden of andere condities van de verleende dienst, met inbegrip van de maatregelen die dienen te worden genomen om de dienst op gecontroleerde wijze stop te zetten.

K5.4 **Niveaus 3 en 4:** Uitgevers van Zweedse eID's dienen op verzoek van het Agentschap voor Digitale Overheid (DIGG) of een andere overeenkomstsluitende partij die afhankelijk is van door de uitgever verleende diensten, informatie te verstrekken over de eigendom en het beheer van het bedrijf.

K5.5 Een uitgever van Zweedse eID's die zijn activiteiten beëindigt, volgt een vooraf vastgesteld plan voor beëindiging van de dienst. Het plan omvat het informeren van alle gebruikers van de dienst en DIGG. De uitgevende instelling houdt verder gearchiveerd materiaal beschikbaar in overeenstemming met K2.7 en K2.8 na beëindiging.

Toepassing

K5.6 Een Zweedse eID mag alleen worden afgegeven op verzoek van de aanvrager of via een andere gelijkwaardige aanvaardingsprocedure, en alleen nadat de aanvrager op de hoogte is gesteld van de voorwaarden waaronder de eID wordt afgegeven en van de verantwoordelijkheid die op hem of haar zal rusten.

De afgifte van een eID die een geldig of recent geblokkeerd eID-document vervangt of aanvult dat eerder door dezelfde uitgevende instelling is afgegeven, kan echter plaatsvinden zonder voorafgaande aanvraagprocedure.

K5.7 Een aanvraag voor een Zweedse eID wordt gekoppeld aan een persoonlijk identiteitsnummer of coördinatienummer, alsmede aan de informatie die de uitgevende instelling anderszins nodig heeft om een dergelijke eID te verstrekken.

Vaststelling van de identiteit van de aanvrager

K5.8 Uitgevers van Zweedse eID's dienen te verifiëren of de informatie die aan de aanvraag is gekoppeld, volledig is en overeenkomt met informatie die in een officieel register is geregistreerd.

K5.9 Wanneer informatie die in een officieel register dient te worden gecontroleerd, als vertrouwelijk is aangemerkt ("beschermde identiteit"), kunnen de nodige controles met andere gelijkwaardige middelen worden uitgevoerd.

K5.10 Identificatie van de aanvrager tijdens een persoonlijk bezoek:

Uitgevers van Zweedse eID's kunnen de identiteit van de aanvrager verifiëren tijdens een persoonlijk bezoek, op dezelfde manier als bij de afgifte van een standaard identiteitsdocument.

K5.11 Identificatie op afstand van de aanvrager in de bestaanderelatie:

Niveau 3 Uitgevers van Zweedse eID's die de aanvrager reeds hebben geïdentificeerd in een relatie waarbij sprake is van economisch of juridisch significante transacties, en waarbij de aanvrager op afstand kan worden geïdentificeerd met andere betrouwbare middelen die gelijkwaardig zijn aan de niveau 3-vereisten van het Zweedse eID-keurmerk, kunnen deze methode gebruiken om de identiteit van de aanvrager vast te stellen.

Niveau 4 Niet van toepassing.

K5.12 Identificatie via Zweedse eID:

Een uitgever van Zweedse eID's kan de aanvrager op afstand identificeren door middel van een bestaande geldige Zweedse eID van ten minste hetzelfde zekerheidsniveau als de eID die dient te worden uitgegeven, indien hij deze identificatie zonder contractuele belemmeringen kan gebruiken als basis voor de afgifte van een nieuwe eID.

Niveau 4 De geldigheidsduur van de nieuw afgegeven eID mag niet langer zijn dan de geldigheidsduur van de bestaande eID.

K5.13 Identificatie op afstand van de aanvrager:

Niveau 2 Uitgevers van Zweedse eID's kunnen betrouwbare beeldopnamen van een geldig standaardidentiteitsdocument en de gezichtsopname van de aanvrager gebruiken als basis voor het op afstand vaststellen van de identiteit van de aanvrager indien de vergelijking geen aanleiding geeft tot twijfels over de ware identiteit van de aanvrager.

Niveau 3 Uitgevers van Zweedse eID's kunnen, door middel van een beveiligde lezing van een geldig standaard identiteitsdocument dat elektronisch opgeslagen

biometrische gegevens bevat, de identiteit van de aanvrager op afstand vaststellen op basis van die gegevens, indien de overeenkomstige biometrische gegevens van de te identificeren persoon op voldoende veilige wijze kunnen worden verzameld, zodat een vergelijking kan worden gemaakt met dezelfde betrouwbaarheid als in het geval van een persoonlijk bezoek, en indien de vergelijking geen aanleiding geeft tot twijfel over de ware identiteit van de aanvrager.

Niveau 4 Niet van toepassing.

Registratie

K5.14 Uitgevers van Zweedse eID's houden, rekening houdend met de toepasselijke regels inzake de bescherming van persoonsgegevens, een register bij van verbonden gebruikers en de toegewezen elektronische identificatiedocumenten, en houden dit register actueel.

6. Afgifte en blokkering van eID

Ontwerp van technische middelen

K6.1 Technische middelen:

Niveaus 2 en 3: Technische middelen voor elektronische identificatie via eID met het Zweedse eID-keurmerk worden ontworpen volgens een tweefactorbeginsel, waarbij het ene deel bestaat uit elektronisch opgeslagen informatie die de gebruiker dient te bewaren, en het andere deel bestaat uit wat de gebruiker dient te gebruiken om de eID te activeren.

Niveau 4 Technische middelen voor elektronische identificatie via eID met het Zweedse eID-keurmerk worden ontworpen volgens een tweefactorbeginsel, waarbij het ene deel bestaat uit een persoonlijke beveiligingsmodule die de gebruiker dient te bezitten, en het andere deel bestaat uit wat de gebruiker dient te gebruiken om de beveiligingsmodule te activeren.

K6.2 Het activeringsmechanisme en de gepersonaliseerde code dienen zodanig te zijn ontworpen dat het onwaarschijnlijk is dat derden de bescherming schenden, zelfs met mechanische middelen.

Niveaus 3 en 4: De bescherming omvat mechanismen om het kopiëren en manipuleren van het elektronische identificatiedocument te voorkomen.

K6.3 Gebruikers van een eID met het Zweedse eID-keurmerk kunnen op eigen initiatief, binnen de geldigheidsduur van de eID, kosteloos en zonder noemenswaardig ongemak een nieuwe persoonlijke code uitwisselen of aanvragen en, via begeleiding of automatische productie, worden geholpen bij het handhaven van de vereisten van K6.2.

Als de eID zodanig is ontworpen dat er geen gepersonaliseerde code kan worden uitgewisseld, dient de gebruiker in plaats daarvan, onder dezelfde voorwaarden, onmiddellijk een nieuwe eID te kunnen verkrijgen met een nieuwe gepersonaliseerde code die de vorige vervangt via een blokkeringsprocedure.

K6.4 Uitgevers van Zweedse eID's zorgen ervoor dat de voor de elektronische identificatie van houders geregistreerde gegevens de aanvrager op unieke wijze vertegenwoordigen en bij de afgifte van het eID-document aan de persoon in kwestie worden toegeschreven.

K6.5 De geldigheidsduur van afgegeven eID's wordt beperkt, rekening houdend met de beveiligingskenmerken van het eID-document en de risico's van misbruik. De maximale geldigheidsduur van de eID is vijf jaar.

Verstrekking van een eID-document

K6.6 Voorziening op afstand:

Niveau 2 Een uitgever van Zweedse eID's verstrekt het e-ID-document op een wijze die de contactgegevens bevestigt die in het officiële register zijn bijgehouden of dergelijke informatie die in verband met de elektronische procedure is geregistreerd overeenkomstig K5.13 niveau 2.

Niveau 3 Een uitgever van Zweedse eID's die een eID verstrekt via een elektronische procedure die in overeenstemming is met K5.11 Niveau 3, K5.12 Niveau 3 of K5.13 Niveau 3, dient er, wanneer deze nieuw wordt afgegeven, afzonderlijk en onafhankelijk van de voorziening op het gebied van beveiliging, voor te zorgen dat de gebruiker ervan in kennis wordt gesteld dat een dergelijk e-ID-document is overhandigd, of door andere maatregelen te zorgen voor een gelijkwaardige mate van controle dat de persoon wordt gewaarschuwd voor het risico van identiteitsdiefstal in verband met de voorziening.

Niveau 4 Een uitgever van Zweedse eID's die een eID verstrekt via een elektronische procedure die voldoet aan K5.12 Niveau 4, dient er, wanneer deze nieuw wordt uitgegeven, afzonderlijk en onafhankelijk van de voorziening op het gebied van beveiliging, voor te zorgen dat de gebruiker ervan in kennis wordt gesteld dat een dergelijk eID-document is overhandigd.

K6.7 Voorziening tijdens een persoonlijk bezoek:

Een uitgever van Zweedse eID's verstrekt tijdens een persoonlijk bezoek en na een identiteitscontrole overeenkomstig K5.10 het elektronische identificatiedocument tegen ondertekend ontvangstbewijs, en verstrekt voorts het deel dat de gebruiker dient te gebruiken om de eID afzonderlijk en onafhankelijk van de verstrekking van het eID-document voor wat betreft beveiliging te activeren, op basis van contactgegevens die in een officieel register worden bijgehouden of andere informatie die even geloofwaardig is.

Blokkeringsdienst

K6.8 Uitgevers van Zweedse eID's dienen een blokkeringsdienst aan te bieden die voor de gebruiker goed toegankelijk is om zijn eID te kunnen blokkeren.

K6.9 Uitgevers van Zweedse eID's dienen verzoeken tot blokkering snel en veilig te verwerken en maatregelen te nemen om systematisch misbruik van de blokkeringsdienst of andere opzettelijke acties die leiden tot de wijdverbreide blokkering van elektronische identificatiedocumenten, te voorkomen, zodat de eID's van gebruikers beschikbaar zijn wanneer dat nodig is

7. Verificatie van elektronische identiteiten van houders

K7.1 Uitgevers van Zweedse eID's zorgen ervoor dat, bij de verificatie van de identiteit van de houder, betrouwbare controles worden uitgevoerd op de echtheid en geldigheid van het eID-document.

K7.2 Uitgevers van Zweedse eID's zorgen ervoor dat er technische beveiligingscontroles zijn uitgevoerd bij het verifiëren van de elektronische identiteiten van houders, zodat het onwaarschijnlijk is dat derden door middel van gissen, afluisteren, opnieuw afspelen of manipuleren van het proces de beschermingsmechanismen kunnen schenden.

8. Afgifte van identiteitsbewijzen

Uitgevers van Zweedse eID's die een dienst verlenen voor de afgifte van identiteitscertificaten aan betrouwbare e-diensten, dienen ook te voldoen aan de bepalingen van dit artikel.

K8.1 Uitgevers van Zweedse eID's zorgen ervoor dat de dienst voor de afgifte van identiteitscertificaten goed toegankelijk is en dat de afgifte van identiteitscertificaten wordt voorafgegaan door een betrouwbare identificatie overeenkomstig de bepalingen van artikel 7.

Niveau 4 Certificaten bevatten een verwijzing naar cryptografisch sleutelmateriaal dat door de uitgever is geverifieerd als zijnde in het uitsluitende bezit van de houder.

K8.2 Ingediende identiteitsbewijzen zijn slechts zo lang geldig als nodig is om de gebruiker toegang te verlenen tot de gevraagde e-dienst, en worden beschermd, zodat de informatie alleen door de beoogde ontvanger kan worden gelezen en de echtheid van de certificaten door de ontvangers van de certificaten kan worden geverifieerd.

K8.3 Uitgevers van Zweedse eID's beperken, rekening houdend met de risico's van misbruik van de certificeringsdienst, de termijn waarbinnen meerdere opeenvolgende identiteitsbewijzen aan een bepaalde houder kunnen worden afgegeven voordat de houder opnieuw wordt geïdentificeerd overeenkomstig de bepalingen van artikel 7.