NÚMERO DO FICHEIRO: 2022-0941
ID DE CLASSIFICAÇÃO: 3.2.3

Quadro de confiança

para a identificação eletrónica sueca

Versão de 4 de outubro de 2022

1. Contexto e finalidade

O quadro de confiança para a identificação eletrónica sueca visa estabelecer requisitos comuns aplicáveis aos emitentes de identificações eletrónicas revistos e aprovados pela Agência Sueca para a Administração Digital (DIGG). Os requisitos dividem-se em diferentes níveis de proteção – conhecidos como níveis de garantia – que correspondem a diferentes graus de segurança técnica e operacional por parte do emitente e diferentes graus de verificação de que a pessoa a quem é emitido um documento de identificação eletrónica é efetivamente quem diz ser.

Os requisitos deste quadro de confiança aplicam-se aos níveis de garantia 2 a 4, correspondendo o nível 4 ao nível mais elevado de proteção.

O cumprimento deve ser interpretado da seguinte forma:

(a) Se o nível de garantia não for especificado, o requisito deve ser cumprido a todos os níveis; e

(b) Se o nível de garantia for especificado, o cumprimento deve ser assegurado, pelo menos, ao nível pertinente.

Os requisitos estabelecidos para um nível inferior ao nível pertinente não são tidos em conta.

2. Organização e governação

Requisitos operacionais gerais

K2.1 Os emitentes de identificações eletrónicas suecas que não sejam organismos públicos devem operar como entidades jurídicas registadas e subscrever e manter o seguro exigido para a atividade.

K2.2 Os emitentes de identificações eletrónicas suecas têm de ter uma empresa estabelecida, estar plenamente operacionais em todas as partes especificadas no presente documento e estar bem familiarizados com os requisitos legais que lhes são impostos enquanto emitentes de identificações eletrónicas suecas.

K2.3 Os emitentes de identificações eletrónicas suecas têm de ter capacidade para suportar o risco de responsabilidade por danos e dispor de recursos financeiros suficientes para realizar as suas operações durante, pelo menos, um ano.

Segurança da informação

K2.4 Os emitentes de identificações eletrónicas suecas devem ter estabelecido um sistema de gestão da segurança da informação (SGSI) para as partes das suas atividades afetadas pelo quadro de confiança, que se baseia, se for caso disso, na norma ISO/IEC 27001 ou em princípios equivalentes para a gestão e o controlo do trabalho de segurança da informação, incluindo o seguinte:

(a) Todos os processos administrativos e técnicos críticos para a segurança têm de ser documentados e basear-se numa base formal, em que as funções, responsabilidades e poderes estejam claramente definidos;

(b) Os emitentes de identificações eletrónicas suecas devem assegurar que disponham permanentemente de recursos humanos suficientes para cumprir as suas obrigações;

(c) Os emitentes de identificações eletrónicas suecas devem estabelecer um processo de gestão dos riscos que, de forma adequada, contínua ou, pelo menos, de 12 em 12 meses, analise as ameaças e vulnerabilidades na empresa e que, através da introdução de medidas de segurança, equilibre os riscos para níveis aceitáveis;

(d) Os emitentes de identificações eletrónicas suecas devem estabelecer um processo de gestão de incidentes que garanta sistematicamente a qualidade do serviço, as formas de comunicação posterior e a adoção de medidas reativas e preventivas adequadas para atenuar ou prevenir os danos resultantes de tais eventos;

(e) Os emitentes de identificações eletrónicas suecas devem estabelecer e testar regularmente um plano de continuidade que cumpra os requisitos de acessibilidade da empresa através da capacidade de restabelecer processos críticos em caso de crise ou incidentes graves;

(f) Os emitentes de identificações eletrónicas suecas devem avaliar regularmente o trabalho de segurança da informação e introduzir medidas de melhoria no sistema de gestão.

K2.5 Âmbito e maturidade do sistema de gestão:

Nível 4: O sistema de gestão da segurança da informação deve cumprir a norma SS-ISO/IEC 27001:2017 ou versões subsequentes ou internacionais equivalentes da norma e, no âmbito desta, incluir todos os requisitos impostos aos emitentes de identificações eletrónicas suecas.

Condições de subcontratação

K2.6 Um emitente de identificações eletrónicas suecas que tenha subcontratado a outra parte a execução de um ou mais processos críticos para a segurança deve definir mediante contrato os processos críticos pelos quais o subcontratante é responsável e os requisitos que lhes são aplicáveis, bem como clarificar a relação contratual na declaração do emitente.

Rastreabilidade, eliminação e armazenamento de documentos

K2.7 Os emitentes de identificações eletrónicas suecas devem armazenar:

(a) Documentos de pedido e documentos relacionados com a emissão, receção ou bloqueio de identificações eletrónicas;

(b) Contratos, documentos de política e declarações do emitente; e

(c) O histórico de tratamento e outra documentação necessária para comprovar o cumprimento dos requisitos impostos aos emitentes de identificações eletrónicas suecas e que permita um acompanhamento que demonstre que os processos e controlos críticos para a segurança estão em vigor e são eficazes.

K2.8 O período de armazenamento não deve ser inferior a cinco anos e o material deve poder ser produzido de forma legível durante todo esse período, a menos que seja necessário um requisito de eliminação do ponto de vista da privacidade e seja apoiado por lei ou outra regulamentação.

Revisão e acompanhamento

K2.9 Os emitentes de identificações eletrónicas suecas devem estabelecer uma função de auditoria interna que reveja periodicamente as atividades de emissão. O auditor interno é independente no exercício das suas funções, de modo que assegure uma análise objetiva e imparcial, e tem a competência e a experiência necessárias para o exercício das suas funções. O auditor interno deve planear de forma independente a realização da auditoria e documentá-la num plano de auditoria que abranja um período de três anos. Os elementos de auditoria devem ser selecionados com base numa análise dos riscos e da materialidade e devem basear-se nas descrições das operações apresentadas pelo emitente à Agência para a Administração Digital.

Níveis 3 e 4: a auditoria interna deve ser realizada com base em normas de auditoria aceites.

3. Segurança física, administrativa e orientada para as pessoas

K3.1 As partes centrais da operação devem estar fisicamente protegidas de danos resultantes de eventos ambientais, acessos não autorizados ou outras perturbações externas. O controlo de acessos deve ser aplicado de modo que o acesso a zonas sensíveis seja limitado ao pessoal autorizado, os suportes de informação sejam armazenados e eliminados de forma segura e o acesso a essas zonas protegidas seja continuamente monitorizado.

K3.2 Antes de uma pessoa assumir qualquer uma das funções identificadas em conformidade com o ponto K2.4, alínea a), e que sejam de especial importância para a segurança, o emitente de identificações eletrónicas suecas deve ter realizado verificações de antecedentes, a fim de garantir que a pessoa pode ser considerada fiável e que possui as qualificações e a formação necessárias para desempenhar de forma segura as tarefas decorrentes da função.

K3.3 Os emitentes devem dispor de procedimentos para assegurar que apenas o pessoal especificamente autorizado tenha acesso aos dados recolhidos e conservados em conformidade com o ponto K2.7.

K3.4 **Níveis 3 e 4:** os emitentes devem assegurar, ao longo de toda a cadeia do processo de emissão, que a separação de funções seja aplicada de modo que nenhuma pessoa possa obter uma identificação eletrónica em nome de outra pessoa.

4. Segurança técnica

K4.1 Os emitentes de identificações eletrónicas suecas devem assegurar que os controlos técnicos em vigor sejam suficientes para alcançar o nível de proteção considerado necessário no que diz respeito à natureza, ao âmbito e a outras circunstâncias da atividade e que esses controlos funcionem e sejam eficazes.

K4.2 Os meios eletrónicos de comunicação utilizados na transmissão de dados sensíveis devem ser protegidos da interceção, manipulação e reprodução.

K4.3 O material de codificação criptográfica sensível utilizado para emitir identificações eletrónicas, identificar titulares e emitir certificados de identidade deve ser protegido de modo que:

(a) O acesso seja limitado, lógica e fisicamente, às funções e aplicações estritamente necessárias;

(b) O material de codificação nunca seja armazenado em texto simples em suportes de armazenamento persistentes;

(c) O material de codificação esteja protegido pela utilização de um módulo de *hardware* criptográfico com mecanismos de segurança ativos que neutralizam as tentativas físicas e lógicas de comprometer o material de codificação;

(d) Os mecanismos de segurança para a proteção do material de codificação sejam transparentes e baseados em normas reconhecidas e bem estabelecidas; e

(e) **Níveis 3 e 4:** os dados de ativação para proteção de material de codificação sejam geridos através de controlo multipessoal.

K4.4 Os emitentes devem dispor de procedimentos documentados para assegurar que o nível de proteção exigido no ambiente informático pertinente possa ser mantido ao longo do tempo e em ligação com as alterações, incluindo avaliações regulares da vulnerabilidade e preparação adequada para fazer face à evolução dos níveis de risco e aos incidentes que ocorram.

5. Pedido, identificação e registo

Informações sobre as condições

K5.1 Os emitentes de identificações eletrónicas suecas devem fornecer informações sobre os contratos, os termos e as condições, bem como informações conexas e quaisquer restrições à utilização do serviço, aos utilizadores conectados, aos prestadores de serviços eletrónicos e a outras pessoas que possam confiar no serviço do emitente.

K5.2 Um emitente de identificações eletrónicas suecas deve referir claramente os termos e condições e conceber os procedimentos de modo que os termos e condições sejam fornecidos ao requerente no processo de emissão.

K5.3 Os emitentes de identificações eletrónicas suecas devem apresentar uma declaração do emitente que inclua:

(a) A identidade e os dados de contacto do emitente;

(b) Breves descrições dos serviços e soluções prestados pelo emitente, incluindo os métodos aplicados para o pedido, emissão e bloqueio;

(c) As condições associadas ao serviço prestado, incluindo as obrigações do utilizador de proteger a sua identificação eletrónica, as obrigações e responsabilidades do emitente, quaisquer garantias dadas e a disponibilidade prometida;

(d) Informações sobre o tratamento de dados pessoais e a forma como é efetuado; e

(e) Disposições para alterar os termos ou outras condições do serviço prestado, incluindo as medidas a tomar para descontinuar o serviço de forma controlada.

K5.4 **Níveis 3 e 4:** os emitentes de identificações eletrónicas suecas devem, mediante pedido da Agência para a Administração Digital (DIGG) ou de outra parte contratante que dependa de serviços prestados pelo emitente, fornecer informações sobre a forma como a empresa é detida e gerida.

K5.5 Um emitente de identificações eletrónicas suecas que cesse as suas atividades deve seguir um plano preestabelecido para a descontinuação do serviço. O plano deve incluir informar todos os utilizadores do serviço e a DIGG. O emitente deve ainda manter material arquivado disponível em conformidade com os pontos K2.7 e K2.8 após a descontinuação.

Pedido

K5.6 Uma identificação eletrónica sueca só pode ser emitida a pedido do requerente ou através de outro procedimento de aceitação equivalente e apenas depois de o requerente ter sido informado das condições em que é emitida e da responsabilidade que lhe será atribuída.

No entanto, a emissão de uma identificação eletrónica que substitua ou complemente um documento de identificação eletrónica válido ou recentemente bloqueado emitido anteriormente pelo mesmo emitente pode ocorrer sem qualquer procedimento de pedido prévio.

K5.7 Um pedido de identificação eletrónica sueca deve estar associado a um número de identificação pessoal ou a um número de coordenação, bem como às informações que são necessárias para que o emitente forneça essa identificação eletrónica.

Determinação da identidade do requerente

K5.8 Os emitentes de identificações eletrónicas suecas têm de verificar se as informações associadas ao pedido estão completas e correspondem às informações registadas num registo oficial.

K5.9 Se as informações a verificar num registo oficial estiverem assinaladas como confidenciais («identidade protegida»), os controlos necessários podem ser efetuados por outros meios equivalentes.

K5.10 Identificação do requerente durante uma visita presencial:

Os emitentes de identificações eletrónicas suecas podem verificar a identidade do requerente durante uma visita presencial, da mesma forma que aquando da emissão de um documento de identidade normalizado.

K5.11 Identificação remota do requerente na relação existente:

Nível 3: os emitentes de identificações eletrónicas suecas que já tenham identificado o requerente numa relação que envolva transações significativas do ponto de vista económico ou jurídico, e em que o requerente possa ser identificado remotamente por outros meios fiáveis equivalentes aos requisitos de nível 3 da marca de qualidade de identificação eletrónica sueca, podem utilizar este método para determinar a identidade do requerente.

Nível 4: não aplicável.

K5.12 Identificação através da identificação eletrónica sueca:

Um emitente de identificações eletrónicas suecas pode identificar o requerente remotamente através de uma identificação eletrónica sueca válida existente com, pelo menos, o mesmo nível de garantia do que a que será emitida, se puder, sem obstáculos contratuais, utilizar essa identificação como base para emitir uma nova identificação eletrónica.

Nível 4: o período de validade da nova identificação eletrónica emitida deve limitar-se a não exceder o período de validade da identificação eletrónica existente.

K5.13 Identificação remota do requerente:

Nível 2: os emitentes de identificações eletrónicas suecas podem utilizar registos de imagem fiáveis de um documento de identidade normalizado válido e a imagem facial do requerente como base para determinar remotamente a identidade do requerente, se a comparação não suscitar dúvidas quanto à verdadeira identidade do requerente.

Nível 3: os emitentes de identificações eletrónicas suecas podem, através de uma leitura segura de um documento de identidade normalizado válido que contenha dados biométricos armazenados eletronicamente, determinar remotamente a identidade do requerente com base nesses dados, se os dados biométricos correspondentes da pessoa a identificar puderem ser recolhidos de forma suficientemente segura para permitir uma comparação com fiabilidade equivalente à de uma visita presencial e se a comparação não suscitar dúvidas quanto à verdadeira identidade do requerente.

Nível 4: não aplicável.

Registo

K5.14 Os emitentes de identificações eletrónicas suecas devem, tendo em conta as regras aplicáveis em matéria de proteção de dados pessoais, manter um registo dos utilizadores conectados e dos documentos de identificação eletrónica atribuídos, e mantê-lo atualizado.

6. Emissão e bloqueio da identificação eletrónica

Conceção de meios técnicos

K6.1 Meios técnicos:

Níveis 2 e 3: os meios técnicos de identificação eletrónica através de identificação eletrónica com a marca de qualidade de identificação eletrónica sueca devem ser concebidos de acordo com um princípio de dois fatores, em que uma parte consiste em informações armazenadas eletronicamente que o utilizador deve deter e a outra parte consiste no que o utilizador deve utilizar para ativar a identificação eletrónica.

Nível 4: os meios técnicos de identificação eletrónica através de identificação eletrónica com a marca de qualidade de identificação eletrónica sueca devem ser concebidos de acordo com um princípio de dois fatores, em que uma parte consiste num módulo de segurança pessoal que o utilizador deve possuir e a outra parte consiste no que o utilizador deve utilizar para ativar o módulo de segurança.

K6.2 O mecanismo de ativação e o código personalizado devem ser concebidos de modo que seja improvável que terceiros violem a proteção, mesmo por meios mecânicos.

Níveis 3 e 4: a proteção deve incluir mecanismos para impedir a cópia e a manipulação do documento de identificação eletrónica.

K6.3 Os utilizadores de identificações eletrónicas com a marca de qualidade de identificação eletrónica sueca devem poder, por sua própria iniciativa, dentro do período de validade da identificação eletrónica, a título gratuito e sem inconvenientes significativos, trocar ou solicitar um novo código pessoal e, através de orientações ou da produção automática, ser ajudados a manter os requisitos do ponto K6.2.

Se a identificação eletrónica for concebida de modo que um código personalizado não possa ser trocado, o utilizador deve, em vez disso, nas mesmas condições, poder obter prontamente uma nova identificação eletrónica com um novo código personalizado que substitua o anterior através de um procedimento de bloqueio.

K6.4 Os emitentes de identificações eletrónicas suecas devem assegurar que os dados registados para identificação eletrónica dos titulares representem exclusivamente o requerente e sejam atribuídos à pessoa em questão aquando da emissão do documento de identificação eletrónica.

K6.5 O período de validade das identificações eletrónicas emitidas deve ser limitado, tendo em conta os elementos de segurança do documento de identificação eletrónica e os riscos de utilização abusiva. O período máximo de validade da identificação eletrónica é de cinco anos.

Fornecimento de um documento de identificação eletrónica

K6.6 Fornecimento remoto:

Nível 2: um emitente de identificações eletrónicas suecas deve fornecer o documento de identificação eletrónica de uma forma que confirme os dados de contacto mantidos no registo oficial ou as informações registadas no âmbito do procedimento eletrónico de acordo com o ponto K5.13, nível 2.

Nível 3: um emitente de identificações eletrónicas suecas que forneça uma identificação eletrónica através de um procedimento eletrónico que esteja em conformidade com o ponto K5.11, nível 3, o ponto K5.12, nível 3, ou o ponto K5.13, nível 3, deve, quando emitida de novo, de forma separada e independente do fornecimento em termos de segurança, assegurar que o utilizador seja informado de que esse documento de identificação eletrónica foi entregue ou assegurar, através de outras medidas, um grau equivalente de controlo de que a pessoa é alertada para o risco de usurpação de identidade relacionado com o fornecimento.

Nível 4: um emitente de identificações eletrónicas suecas que forneça uma identificação eletrónica através de um procedimento eletrónico conforme com o ponto K5.12, nível 4, deve, quando emitida de novo, de forma separada e independente do fornecimento em termos de segurança, assegurar que o utilizador seja informado de que esse documento de identificação eletrónica foi entregue.

K6.7 Fornecimento durante uma visita presencial:

Um emitente de identificações eletrónicas suecas deve, durante uma visita presencial e após um controlo de identidade em conformidade com o ponto K5.10, fornecer o documento de identificação eletrónica contra recibo assinado, bem como fornecer a parte que o utilizador deve utilizar para ativar a identificação eletrónica de forma separada e independente do fornecimento do documento de identificação eletrónica em termos de segurança, com base nos dados de contacto mantidos num registo oficial ou noutras informações de credibilidade equivalente.

Serviço de bloqueio

K6.8 Os emitentes de identificações eletrónicas suecas devem prestar um serviço de bloqueio com boa acessibilidade para que o utilizador possa bloquear a sua identificação eletrónica.

K6.9 Os emitentes de identificações eletrónicas suecas devem tratar e efetuar de forma rápida e segura os pedidos de bloqueio e tomar medidas para evitar a utilização abusiva sistemática do serviço de bloqueio ou outras ações intencionais que conduzam ao bloqueio generalizado dos documentos de identificação eletrónica, assegurando que as identificações eletrónicas dos utilizadores estejam disponíveis quando necessário

7. Verificação das identidades eletrónicas dos titulares

K7.1 Os emitentes de identificações eletrónicas suecas devem assegurar que, ao verificar a identidade do titular, sejam efetuados controlos fiáveis da autenticidade e validade do documento de identificação eletrónica.

K7.2 Os emitentes de identificações eletrónicas suecas devem assegurar que tenham sido implementados controlos técnicos de segurança aquando da verificação das identidades eletrónicas dos titulares, de modo que seja improvável que terceiros, através de adivinhação, escuta, repetição ou manipulação do processo, possam violar os mecanismos de proteção.

8. Emissão de certificados de identidade

Os emitentes de identificações eletrónicas suecas que prestam um serviço de emissão de certificados de identidade a serviços eletrónicos fiáveis devem também cumprir as disposições da presente secção.

K8.1 Os emitentes de identificações eletrónicas suecas devem assegurar que o serviço de emissão de certificados de identidade tenha boa acessibilidade e que a emissão de certificados de identidade seja precedida de uma identificação fiável, em conformidade com o disposto na secção 7.

Nível 4: Os certificados devem incluir uma referência ao material de codificação criptográfica verificado pelo emitente como estando na posse exclusiva do titular.

K8.2 Os certificados de identidade apresentados são válidos apenas durante o tempo necessário para permitir ao utilizador o acesso ao serviço eletrónico solicitado, e devem ser protegidos de modo que as informações só possam ser lidas pelo destinatário previsto e que a autenticidade dos certificados possa ser verificada pelos destinatários dos certificados.

K8.3 Os emitentes de identificações eletrónicas suecas devem, tendo em conta os riscos de utilização abusiva do serviço de certificação, limitar o período durante o qual podem ser emitidos vários certificados de identidade consecutivos a um determinado titular antes de este ser reidentificado em conformidade com o disposto na secção 7.