Déclaration de pratiques de la Zürcher Kantonalbank

Délivrance de certificats qualifiés | Mai 2024

Documents de base

ETSI EN 119 461	Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for trust service components providing identity proofing of trust service subjects
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques, RS 943.03
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique et des autres applications de certificats numériques, RS 943.032

1 Objet et contenu du présent document

La Zürcher Kantonalbank (ZKB) offre à un cercle de personnes (« utilisateurs ») désignées par elle et ayant une relation commerciale avec elle la possibilité de signer certains documents électroniquement de manière qualifiée. La signature électronique qualifiée (« SEQ ») répond aux exigences de sécurité les plus élevées et, associée à un horodatage qualifié, est assimilée à la signature manuscrite.

La présente déclaration de pratiques informe les utilisateurs et les autres parties impliquées sur la manière d'effectuer l'identification et l'association au certificat qualifié pour la SEQ.

2 Utilisation de logiciels et/ou de services de tiers

Pour l'identification et l'association à un certificat qualifié, la ZKB peut utiliser des logiciels et/ou des services tiers. En principe et sauf avis contraire, leur utilisation s'effectue sous la responsabilité de la ZKB.

Les tiers qui fournissent des logiciels ou des services pour la SEQ sont également tenus de se conformer aux exigences réglementaires de la SCSE et des normes ETSI. Lors de l'évaluation de ces tiers, la ZKB a vérifié qu'ils répondaient aux exigences et normes correspondantes. Elle s'assure que ces exigences et normes seront également respectées à l'avenir.

3 Procédure de délivrance d'un certificat qualifié

Les conditions préalables à l'utilisation d'une SEQ peuvent être divisées en deux sous-processus :

3.1 Identification (en ligne)

La ZKB obtient de l'utilisateur des photos de toutes les pages pertinentes de son document d'identification et de lui-même. Elle compare la photo prise par l'utilisateur avec la photo du document d'identification. A l'aide d'outils techniques appropriés permettant au moins la lecture et le déchiffrement des informations dans la zone de lecture automatique, la ZKB compare les informations déchiffrées avec les autres informations figurant sur la pièce d'identité et avec les données indiquées par l'utilisateur.

Elle évalue l'authenticité du document d'identification au moyen d'au moins deux caractéristiques de sécurité choisies au hasard. De plus, la ZKB s'assure que la photo de l'utilisateur a été créée lors de la procédure d'identification.

Une liste des documents d'identification autorisés pour l'identification en ligne est disponible sur zkb.ch.

3.2 Délivrance d'un certificat qualifié pour la SEQ

Une fois l'identification réussie, un certificat qualifié peut être délivré pour la SEQ.

Pour ce faire, la ZKB transmet à un prestataire de services de certification les données nécessaires issues de l'identification. Avec les données de l'identification, le prestataire de services de certification délivre un certificat qualifié pour la SEQ et les utilisateurs peuvent ensuite utiliser le certificat qualifié pour signer électroniquement certains documents dans le cadre de leur relation commerciale avec la ZKB.

Les documents signés électroniquement ont la même validité que les documents signés à la main et sont assimilés à leur original.

4 Déclaration d'invalidité d'un certificat qualifié

4.1 Raisons

Le prestataire de services de certification peut déclarer un certificat qualifié invalide pour les raisons suivantes (les documents signés électroniquement jusqu'à cette date restent valablement signés) :

1. Il soupçonne que la clé privée ou d'autres données chiffrées pour la création de la signature ont été compromises, volées, divulguées ou utilisées de manière abusive.

2. L'utilisateur n'a plus besoin du certificat qualifié.
3. Les données utilisées pour le certificat qualifié ont changé ou ne sont plus correctes, par exemple en raison d'un changement de nom.
4. Au bout de cinq ans (à compter de l'identification réussie), la ZKB déclare de son propre chef qu'un certificat qualifié n'est plus valable.
5. ZKB ou le prestataire de services de certification apprend qu'un certificat qualifié doit être invalidé.

La ZKB peut également demander l'invalidation au prestataire de services de certification si elle prend connaissance de l'un des motifs susmentionnés.

Si les utilisateurs souhaitent obtenir un nouveau certificat qualifié après une déclaration d'invalidité, ils peuvent s'en faire délivrer un à condition de passer à nouveau par une procédure d'identification.

Cette liste n'est pas exhaustive et d'autres motifs peuvent entraîner l'invalidation d'un certificat qualifié par le prestataire de services de certification ou la demande par la ZKB d'une telle invalidation au prestataire de services de certification.

4.2 Restrictions

4.2.1 Conditions requises pour la délivrance de certificats qualifiés

Afin de pouvoir augmenter la sécurité lors de la délivrance de certificats qualifiés, la ZKB se réserve le droit d'imposer des conditions techniques au smartphone utilisé pour la confirmation, par exemple :

1. Exigences relatives au système d'exploitation : pour la délivrance de certificats réglementés, les systèmes d'exploitation suivants sont requis en tant que conditions minimales (état mars 2024) :
    1. Android : Android 6
    2. iOS : iOS 14
2. Pas de smartphone rooté/débridé : l'utilisation d'un smartphone avec des droits système complets (rooté, débridé) n'est pas autorisée pour la délivrance de certificats réglementés et n'est pas autorisée par la ZKB.
3. Biométrie activée : seuls les smartphones avec biométrie activée peuvent être utilisés pour délivrer des certificats réglementés. Si un utilisateur n'a pas activé cette fonction, il est invité à enregistrer ses données biométriques sur le smartphone avant la première utilisation.

Si nécessaire, la ZKB peut modifier les exigences minimales. Elle communiquera les changements correspondants par le biais d'une mise à jour de la déclaration de pratiques.

4.2.2 Utilisation prévue des certificats qualifiés délivrés

Les certificats qualifiés délivrés par le prestataire de services de certification dans le cadre de ce processus ne peuvent être utilisés que dans le cadre des relations commerciales avec la ZKB.

5 Arrêt de l'exploitation (Business Termination)

5.1 Information

Si la ZKB décide de ne plus faire émettre de certificats qualifiés par le prestataire de services de certification, elle prendra les mesures suivantes :

1. Information aux utilisateurs : les utilisateurs qui ont demandé la délivrance d'un certificat qualifié pour une SEQ dans le cadre de leur relation commerciale avec la ZKB sont informés à un moment approprié de la fin de l'utilisation des certificats auprès de la ZKB afin qu'ils puissent prendre leurs dispositions.

2. Information aux tiers impliqués : les tiers impliqués dans le processus d'identification ou dans la délivrance des certificats qualifiés ou de la SEQ sont informés de la cessation de la délivrance et de l'acceptation de certificats avec une préavis approprié.
3. Information à l'organisme d'accréditation et à l'organisme de reconnaissance : l'organisme d'accréditation suisse et l'organisme de reconnaissance accrédité qui contrôle le processus de délivrance des certificats de SEQ sont informés au préalable que la ZKB ne fait plus délivrer de certificats réglementés par l'intermédiaire du prestataire de services de certification. De plus, ils sont informés de la procédure à suivre pour les certificats délivrés jusqu'à cette date.

5.2 Traitement des documents d'identification et des certificats qualifiés

La ZKB est tenue d'archiver les documents d'identification délivrés pendant la période prescrite par la loi et de les présenter sur demande aux personnes ou organismes autorisés. Le prestataire de services de certification est également tenu de conserver les certificats qualifiés délivrés de manière appropriée pendant la période prescrite par la loi.

A compter de la date de cessation de la SEQ, les certificats qualifiés encore en vigueur à ce moment-là sont révoqués par le prestataire de services de certification et aucun autre document ne peut être signé électroniquement à l'aide de ces certificats.

6 Gestion de la sécurité concernant le matériel et les logiciels informatiques utilisés

Les évaluations de sécurité des systèmes informatiques de la ZKB, qu'ils soient internes ou externalisés auprès de tiers, se basent sur la norme ISO 27002 et sont complétées par des mesures issues du NIST Cybersecurity Framework (National Institute of Standards and Technology). Les évaluations de sécurité sont mises à jour au moins une fois par an pour les systèmes informatiques essentiels. Des évaluations de sécurité sont effectuées en cours d'année en cas de modification des processus ou des systèmes informatiques ou sur la base d'analyses d'événements, de révisions/d'audits et d'autres critères de déclenchement.

L'élargissement des champs d'action identifiés est mis en œuvre et surveillé dans le cadre d'un programme sous la forme d'une feuille de route pour la cybersécurité.

7 Entrée en vigueur et modifications

7.1 Entrée en vigueur

La présente déclaration de pratiques entrera en vigueur en mai 2024.

7.2 Modification du présent document

Le présent document sera vérifié à l'occasion de chaque modification significative du service, mais au moins une fois par an, pour s'assurer de son actualité. Il est approuvé par la personne responsable du processus SEQ (responsable de la chaîne de processus) et un membre de la direction, puis mis à la disposition des utilisateurs sur zkb.ch.