Practice Statement der Zürcher Kantonalbank

Über die Ausstellung von qualifizierten Zertifikaten | Mai 2024

Grundlagen-Dokumente

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
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, SR 943.03
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, SR 943.032

1 Zweck und Inhalt dieses Dokuments

Die Zürcher Kantonalbank (ZKB) bietet einem von ihr bestimmten Personenkreis («Nutzer») und im Zusammenhang mit einer Geschäftsbeziehung mit der ZKB die Möglichkeit an, ausgewählte Dokumente qualifiziert elektronisch zu signieren. Die qualifizierte elektronische Signatur («QES») entspricht den höchsten Sicherheitsanforderungen und ist, in Verbindung mit einem qualifizierten Zeitstempel, der handschriftlichen Unterschrift gleichgestellt.

Dieses Practice Statement informiert die Nutzer sowie weitere involvierte Parteien über die Durchführung der Identifikation und die Verknüpfung mit dem qualifizierten Zertifikat für die QES.

2 Einsatz von Software und/oder Dienstleistungen Dritter

Für die Durchführung der Identifikation sowie die Verknüpfung mit einem qualifizierten Zertifikat kann die ZKB Software und/oder Dienstleistungen Dritter nutzen. Deren Einsatz folgt grundsätzlich und sofern nicht anderweitig kommuniziert unter Verantwortung der ZKB.

Dritte, die Software oder Dienstleistungen für die QES zur Verfügung stellen, sind ebenfalls verpflichtetet, die regulatorischen Vorgaben und Standards von ZertES und ETSI einzuhalten. Die ZKB hat bei der Evaluierung dieser Dritten geprüft, dass diese die entsprechen Vorgaben und Standards erfüllen und stellt sicher, dass auch in Zukunft diese Vorgaben und Standards eingehalten werden.

3 Ablauf für die Ausstellung eines qualifizierten Zertifikats

Die Voraussetzungen für den Einsatz einer QES können in die beiden folgenden Teil-Prozesse aufgeteilt werden:

3.1 (Online-)Identifikation

Die ZKB holt von dem Nutzer Lichtbilder von allen relevanten Seiten seines Identifizierungsdokuments und von ihm selbst ein. Sie prüft die Übereinstimmung des erstellten Lichtbilds des Nutzers mit dem Lichtbild des Identifizierungsdokuments. Mit Unterstützung geeigneter technischer Hilfsmittel, welche mindestens das Auslesen und Entschlüsseln der Informationen in der Machine Readable Zone erlauben, prüft die ZKB die Übereinstimmung der entschlüsselten Informationen mit den restlichen Angaben auf dem Ausweis und mit den von dem Nutzer angegebenen Daten.

Die ZKB beurteilt die Echtheit des Identifizierungsdokuments anhand von mindestens zwei zufällig ausgewählten Sicherheitsmerkmalen. Zudem stellt die ZKB sicher, dass das Lichtbild des Nutzers im Rahmen des Identifizierungsvorgangs erstellt worden ist.

Eine Liste der zugelassenen Identifizierungsdokumente für die Online-Identifikation ist auf zkb.ch einsehbar.

3.2 Ausstellen eines qualifizierten Zertifikats für QES

Im Anschluss an die erfolgreich durchgeführte Identifikation kann ein qualifiziertes Zertifikat für die QES ausgestellt werden.

Die ZKB übermittelt dazu die notwendigen Daten aus der Identifikation an eine Anbieterin von Zertifizierungsdiensten. Die Anbieterin von Zertifizierungsdiensten stellt mit den Angaben aus der Identifikation ein qualifiziertes Zertifikat für die QES aus und die Nutzer können im Anschluss das qualifizierte Zertifikat verwenden, um – im Rahmen der Geschäftsbeziehung mit der ZKB – ausgewählte Dokumente elektronisch zu signieren.

Elektronisch signierte Dokumente haben dieselbe Wirkung wie handschriftlich unterzeichnete und verkörpern das Original des Dokuments.

4 Ungültigkeitserklärung eines qualifizierten Zertifikats

4.1 Gründe

Bei den folgenden Gründen wird das qualifizierte Zertifikat durch die Anbieterin von Zertifizierungsdiensten für ungültig erklärt, die bis zu diesem Zeitpunkt elektronisch signierten Dokumente bleiben weiterhin rechtsgültig signiert.

1. Es besteht der Verdacht, dass der private Schlüssel oder sonstige verschlüsselte Daten für die Signaturerstellung kompromittiert, gestohlen, offengelegt oder anders missbräuchlich verwendet wurden.
2. Das qualifizierte Zertifikat wird vom Nutzer nicht mehr benötigt.
3. Daten, die für das qualifizierte Zertifikat verwendet werden, ändern sich oder sind nicht mehr korrekt, z. B. aufgrund einer Namensänderung.
4. Nach fünf Jahren (Startzeitpunkt ist die erfolgreich durchlaufene Identifikation) erklärt die ZKB ein qualifiziertes Zertifikat von sich aus für ungültig.
5. Die ZKB oder die Anbieterin von Zertifizierungsdiensten erlangt Kenntnis davon, dass ein qualifiziertes Zertifikat für ungültig zu erklären ist.

Die ZKB kann bei Kenntnisnahme einer der oben aufgeführten Gründe ebenfalls die Ungültigerklärung bei der Anbieterin von Zertifizierungsdiensten beantragen.

Möchten Nutzer nach einer Ungültigkeitserklärung wieder ein qualifiziertes Zertifikat erlangen, können sie sich erneut ein solches Zertifikat ausstellen lassen, wenn sie zuvor wieder eine Identifikation durchlaufen.

Diese Liste ist nicht abschliessend und es können weitere Gründe auftreten, aufgrund derer die Anbieterin von Zertifizierungsdiensten qualifizierte Zertifikate für ungültig erklären wird, resp. die ZKB die Ungültigkeitserklärung bei der Anbieterin von Zertifizierungsdiensten beantragen wird.

4.2 Einschränkungen

4.2.1 Voraussetzungen für die Ausstellung von qualifizierten Zertifikaten

Um die Sicherheit bei der Ausstellung von qualifizierten Zertifikaten erhöhen zu können, behält sich die ZKB vor, technische Voraussetzungen an das für die Bestätigung verwendete Smartphone zu stellen, z. B.:

1. Anforderung an das Betriebssystem: Für das Ausstellen von geregelten Zertifikaten sind die folgenden Betriebssysteme als Mindestvoraussetzungen erforderlich (Stand März 2024):
    1. Android: Android 6
    2. iOS: iOS 14
2. Keine rooted/jailbreaked Smartphone: Das Verwenden von einem Smartphone mit vollen Systemrechten (rooted, jailbreaked) ist für das Ausstellen von geregelten Zertifikaten nicht zulässig und wird durch die ZKB nicht gestattet.
3. Aktivierte Biometrie: Nur Smartphones mit aktivierter Biometrie können für das Ausstellen von geregelten Zertifikaten verwendet werden. Hat ein Nutzer das Feature nicht aktiviert, wird er vor der ersten Nutzung aufgefordert, seine biometrische Daten auf dem Smartphone zu hinterlegen.

Die Mindestanforderungen können durch die ZKB bei Bedarf angepasst werden. Änderungen werden über eine Aktualisierung des Practice Statements kommuniziert.

4.2.2 Verwendungszweck ausgestellter qualifizierter Zertifikate

Die im Rahmen dieses Prozesses durch die Anbieterin von Zertifizierungsdiensten ausgestellten qualifizierten Zertifikate können nur für die Geschäftsbeziehung mit der ZKB verwendet werden.

5 Einstellung des Betriebs (Business Termination)

5.1 Information

Entscheidet sich die ZKB, keine weiteren qualifizierten Zertifikate durch die Anbieterin von Zertifizierungsdiensten mehr ausstellen zu lassen, wird sie die folgenden Massnahmen ergreifen:

1. Information an Nutzer: Nutzer, die ein qualifiziertes Zertifikat für eine QES im Zusammenhang mit der Geschäftsbeziehung mit der ZKB haben ausstellen lassen, werden zu einem geeigneten Zeitpunkt über die Beendigung der Zertifikatsnutzung bei der ZKB informiert, so dass sie eigene Massnahmen treffen können.
2. Information an beteiligte Dritte: Dritte, die an dem Prozess der Identifikation oder bei der Ausstellung des qualifizierten Zertifikates oder der QES- beteiligt sind, werden mit einer geeigneten Frist über die Aufgabe der Zertifikats-Ausstellung und -Akzeptanz informiert.
3. Information an die Akkreditierungsstelle und an die Anerkennungsstelle: Die schweizerische Akkreditierungsstelle und die akkreditierte Anerkennungsstelle, die den Prozess für die Ausstellung eines QES-Zertifikats kontrolliert, werden im Vorfeld darüber informiert, dass die ZKB keine geregelten Zertifikate mehr über die Anbieterin von Zertifizierungsdiensten ausstellen lässt. Zusätzlich werden sie über das weitere Vorgehen für die bis zu diesem Zeitpunkt ausgestellten Zertifikate informiert.

5.2 Handhabung von Identifikationsunterlagen und von qualifizier Zertifikate

Die ZKB ist verpflichtet, die ausgestellten Identifikationsunterlagen für den gesetzlich vorgeschriebenen Zeitraum zu archivieren und auf Nachfrage berechtigten Personen oder Stellen vorzulegen. Die Anbieterin von Zertifizierungsdiensten ist verpflichtet, die ausgestellten qualifizierten Zertifikate für den gesetzlich vorgeschriebenen Zeitraum ebenfalls auf eine geeignete Art und Weise sicherstellen.

Ab dem Zeitpunkt der Aufgabe der QES werden durch die Anbieterin von Zertifizierungsdiensten die zu diesem Zeitpunkt noch gültigen qualifizierten Zertifikate widerrufen und es können mit diesen Zertifikaten keine weiteren Dokumente elektronisch signiert werden.

6 Sicherheitsmanagement bezüglich der verwendeten IT-Hardware und -Software

Die Sicherheitsassessments für IT-Systeme der ZKB, sowohl für interne als auch für ausgelagerte IT-Systeme bei Dritten, basieren auf dem ISO 27002 Standard und werden ergänzt durch Massnahmen aus dem NIST Cybersecurity Framework (National Institute of Standards and Technology). Die Sicherheitsassessments werden für kritische IT-Systeme mindestens einmal jährlich aktualisiert. Unterjährige Sicherheitsassessments erfolgen, wenn Prozesse oder IT-Systeme wesentlich verändert werden oder aufgrund von Ereignisanalysen, Revisionen/Audits und weiteren Anstosskriterien.

Die Weiterentwicklung identifizierter Handlungsfelder wird als Programm in Form einer Cybersecurity Roadmap vollzogen und überwacht.

7 Inkrafttreten & Änderungen

7.1 Inkrafttreten

Dieses Practice Statement tritt per Mai 2024 in Kraft.

7.2 Änderung dieses Dokuments

Dieses Dokument wird mit jeder massgeblichen Anpassung der Dienstleistung, aber mindestens einmal jährlich auf seine Aktualität überprüft, von der für den QES-Prozess verantwortlichen Person (Prozesskettenverantwortliche) und einem Geschäftsleitungs-Mitglied abgenommen und anschliessend den Nutzern auf zkb.ch zugänglich gemacht.