Auszug aus dem Protokoll des Stadtrats von Zürich

vom 22. Januar 2020

58.
Organisation und Informatik, Richtlinie «Standards für den Einsatz digitaler Zertifikate – Städtische Zertifikatsdienste und Anwendungsfälle mit digitalen Zertifikaten», Genehmigung

IDG-Status: öffentlich

1. Zweck

Mit diesem Beschluss soll die städtische Richtlinie «Standards für den Einsatz digitaler Zertifikate – Städtische Zertifikatsdienste und Anwendungsfälle mit digitalen Zertifikaten» (Richtlinie) genehmigt und für die Stadt verbindlich erklärt werden.

2. Ausgangslage

Digitale Zertifikate bilden immer häufiger einen wichtigen Bestandteil bei der Absicherung der elektronischen Kommunikation oder der Digitalisierung von Geschäftsprozessen, z. B. beim elektronischen Signieren von Dokumenten oder Freigaben, bei der eindeutigen Identifizierung von Kommunikationspartnerinnen und -partnern oder beim Verschlüsseln von Daten. Die Ausstellung, Verteilung, Überprüfung und der Rückzug von digitalen Zertifikaten erfolgt durch einen zentralen Zertifizierungsdienst, einer sogenannten Public-Key-Infrastruktur (PKI):

– Qualifizierte (für natürliche Personen) und geregelte Zertifikate (für natürliche Personen oder Unternehmen / Organisationen) sind kostenpflichtig und können gemäss Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES, SR 943.03) nur durch anerkannte Anbieterinnen von Zertifizierungsdiensten – aktuell sind dies die vier Unternehmen Swisscom (Schweiz) AG, QuoVadis, Trustlink Schweiz AG, SwissSign AG und das Bundesamt für Informatik und Telekommunikation BIT – ausgestellt werden.

– Die städtische Public-Key-Infrastruktur erlaubt ausschliesslich die Ausstellung und Verwaltung von internen digitalen Zertifikaten, qualifizierte und geregelte digitale Zertifikate können nicht ausgestellt werden. In internen Anwendungsfällen reichen die städtischen digitalen Zertifikate grundsätzlich aus.

3. Inhalt der Richtlinie

Mit der Verbindlicherklärung der Richtlinie werden die Geschäftsprozess- und IT-Verantwortlichen der Departemente und Dienstabteilungen verpflichtet, beim Einsatz digitaler Zertifikate jeglicher Art – wenn immer möglich – die zentral bereitgestellten städtischen Zertifikatsdienste zu verwenden und sich an die Regelungen der Richtlinie zu halten.

Die Richtlinie umfasst u. a. Folgendes:

– Sie definiert stadtweit verbindlich die unterschiedlichen Begriffe, verschafft einen Überblick über die städtischen Zertifikatsdienste und regelt den stadtweiten Einsatz von digitalen Zertifikaten und die verschiedenen Anwendungsfälle für elektronische Signaturen und zertifikatsbasierte Authentisierungen und Verschlüsselungen.

– Sie weist darauf hin, dass bei einer geplanten Digitalisierung von Geschäftsprozessen und dem Einsatz digitaler Zertifikate in jedem Fall vorgängig rechtlich abzuklären ist, ob seitens Bund, Kanton oder Stadt Zürich Gesetze, Verordnungen oder andere bereichsspezifische Erfordernisse bestehen, die einer Digitalisierung entgegenstehen würden. Diese

rechtlichen Abklärungen werden in die Verantwortung der Organisationseinheiten (zuständiger Rechtsdienst oder Fachjuristinnen und -juristen) übertragen.

– Sie legt fest, dass die Verantwortung für den sicheren Betrieb der zentralen städtischen Zertifikatsdienste, für die Anpassung und Erweiterung mit ähnlichen Zertifikatsdienstleistungen sowie für die Bereitstellung von Information über die zur Verfügung gestellten Services bei der Organisation und Informatik (OIZ) liegt.

Die auch im Rahmen der elektronischen Signatur wichtige Überprüfung der Identität von internen und externen Mitarbeitenden liegt unverändert bei den zuständigen Stellen der Organisationseinheiten (gemäss «Handbuch Informationssicherheit der Stadt Zürich»).

Der Fachstelle Informationssicherheit der OIZ wird die Verantwortung für die Erstellung, Umsetzung, Pflege und Überprüfung aller im Umfeld städtischer Zertifikatsdienste geltenden Regelungen sowie für die Anpassung und regelmässige Überprüfung und Aktualisierung der Richtlinie übertragen. Dabei gilt, dass kleinere Anpassungen durch die Fachstelle Informationssicherheit unter Einbezug der zuständigen städtischen Fachbereiche (z. B. Finanzen, HR, IT) in eigener Kompetenz vorgenommen werden dürfen, grundlegende Änderungen aber einer Genehmigung des Stadtrats bedürfen. Über Änderungen wird ein Nachweis geführt, die entsprechenden Informationen erfolgen im städtischen Intranet.

4. Kosten

Durch diesen Beschluss werden keine finanziellen Mittel bewilligt. Allfällig nötige Massnahmen werden vielmehr projektbezogen konkretisiert und deren Ausgaben gemäss geltender Kompetenzordnung bewilligt.

5. Zuständigkeiten

Dadurch, dass die Richtlinie als stadtweit anwendbar erklärt wird, liegt die Beschlussfassung in Anwendung von Art. 49 Gemeindeordnung (AS 101.100) in der Zuständigkeit des Stadtrats.

Auf Antrag des Vorstehers des Finanzdepartements beschliesst der Stadtrat:

1. Die Richtlinie «Standards für den Einsatz digitaler Zertifikate – Städtische Zertifikatsdienste und Anwendungsfälle mit digitalen Zertifikaten» (Beilage, datiert vom 5. Dezember 2019) wird genehmigt und für die Stadtverwaltung als verbindlich erklärt.
2. Die städtischen Zertifikatsdienste werden durch die OIZ betrieben; die Departemente und Dienstabteilungen werden verpflichtet, beim Bedarf an Zertifikatsdienstleistungen grundsätzlich diese Dienste einzusetzen.
3. Die Klärung der Rechtslage bei einer geplanten Digitalisierung bestehender Geschäftsprozesse und dem Einsatz digitaler Zertifikate und elektronischer Signaturen liegt in der Verantwortung der betroffenen Organisationseinheit.
4. Die Fachstelle Informationssicherheit der OIZ wird beauftragt, die Richtlinie regelmässig zu aktualisieren und bei grundlegenden Änderungen dem Stadtrat zur Genehmigung vorzulegen.
5. Mitteilung je unter Beilage an die Departemente und Dienstabteilungen, die Stadtschreiberin, den Rechtskonsulenten, die Finanzkontrolle und den Datenschutzbeauftragten.

Für getreuen Auszug
die Stadtschreiberin

Dr. Claudia Cuche-Curti