Telefon: 233 - 76 77 77 **IT-Referat**

Digitaler Ausweis

Digitaler Ausweis
Antrag Nr. 20-26 / A 01952 von Frau StRin Dr. Evelyne Menges, Frau StRin Sabine Bär
vom 30.09.2021, eingegangen am 30.09.2021

Sitzungsvorlage Nr. 20-26 / V 05721

2 Anlagen

- Stadtratsantrag
- Stellungnahmen

Beschluss des IT-Ausschusses vom 06.04.2022 (VB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag des Referenten 1
Zusammenfassung 1
1. Einordnung in den Kontext digitaler Identitäten 2
2. Digitale Identitäten 3
3. Digitale Mitarbeiter*innenausweise 3
4. QR-code basierte digitale Ausweise 5
5. Fazit 5
6. Beteiligungen/ Stellungnahmen der Referate 5
II. Antrag des Referenten 6
III. Beschluss 6

I. Vortrag des Referenten

Zusammenfassung

Im vorliegenden Stadtratsantrag mit dem Titel Digitaler Ausweis wird beantragt, dass die Landeshauptstadt München digitale Ausweise für Stadträt*innen, BA-Mitglieder und städtische Mitarbeitende einführt, die nicht nur auf städtischen Endgeräten, sondern auch auf privaten Endgeräten nutzbar sein sollen. Zur Begründung wird angeführt, dass sich Stadträt*innen, BA-Mitglieder und städtische Mitarbeitende in zahlreichen Fällen ausweisen müssen. Hierfür sollen die bislang ausgestellten analogen Ausweise zusätzlich durch digitale Ausweise ergänzt werden, die ähnlich wie der digitale Impfpass auf dem Smartphone gespeichert werden können.

Im Folgenden wird der Antrag in den Kontext Digitaler Identitäten eingebettet und die entsprechenden Aktivitäten der LHM werden dargestellt und erläutert. Die LHM verfolgt dabei den Ansatz, die Mitarbeitenden mit Security-Token auszustatten, über die Zugriffe auf die IT-Systeme der LHM sicher und kryptographisch basiert ermöglicht werden. Diese Token können auch Stadträt*innen oder BA-Mitgliedern ausgehändigt werden, wenn sie den Zugriff auf interne IT-Systeme benötigen. Der im Antrag geforderte digitale Ausweis als zusätzliche Lösung wird aus wirtschaftlicher Sicht für nicht umsetzbar und realisierbar erachtet. Kosten und Nutzen stehen in keinem sinnvollen Verhältnis. Vielmehr verfolgt die LHM weiterhin den eingeschlagenen Weg, mittels der gewählten Security-Token einen sicheren und nutzerfreundlichen Zugang zur IT-Infrastruktur anzubieten und für die rein visuelle Überprüfung von Identität und Funktion weiterhin den analogen Dienstausweis zu verwenden.

1. Einordnung in den Kontext digitaler Identitäten

Im vorliegenden Stadtratsantrag mit dem Titel Digitaler Ausweis wird beantragt, dass die Landeshauptstadt München digitale Ausweise für Stadträt*innen, BA-Mitglieder und städtische Mitarbeitende einführt, die nicht nur auf städtischen Endgeräten, sondern auch auf privaten Endgeräten nutzbar sein sollen. Zur Begründung wird angeführt, dass sich Stadträt*innen, BA-Mitglieder und städtische Mitarbeitende in zahlreichen Fällen ausweisen müssen. Hierfür sollen die bislang ausgestellten analogen Ausweise zusätzlich durch digitale Ausweise ergänzt werden, die ähnlich wie der digitale Impfpass auf dem Smartphone gespeichert werden können.

Es ist also das Ziel der Antragsteller*innen, Stadträt*innen, BA-Mitglieder und Mitarbeitende mit digitalen Ausweisen auszustatten, anhand derer sich die Ausweisinhaber*innen in ihrer Funktion und/oder ihrer Person ausweisen können. Und dies soll unterschiedlichen Stellen gegenüber möglich sein. Es ist nicht eindeutig klar, ob diese Identifikation nur natürlichen Personen gegenüber oder auch IT-Systemen gegenüber stattfinden soll, wie es üblicherweise bei digitalen Identitäten der Fall ist. Im Folgenden werden daher kurz die Themen Digitale Identitäten und Digitale Ausweise für Mitarbeitende aus Sicht der LHM diskutiert und die Aktivitäten der LHM in diesen Bereichen dargestellt, bevor daraus ein Fazit für die Behandlung des Antrags folgt.

Nicht zuletzt auch aus der aktuellen Diskussion um die Impfausweise ist bekannt, dass digitale Ausweise gewisse Eigenschaften erfüllen müssen, um sinnvoll einsetzbar zu sein. Wesentliche Eigenschaften sind:

1. Die Ausweise müssen in gewissem Maße fälschungssicher sein. Das Maß hängt hierbei von den Anforderungen an die Sicherheit und damit die Funktion des Ausweises ab.
2. Es muss gewährleistet sein, dass nur die berechtigte Person den ihr zugeordneten Ausweis zum vorgesehenen Zweck verwenden kann.
3. Die überprüfende Stelle, der der Ausweis vorgelegt wird, muss in der Lage sein, die Echtheit und die korrekte Anwendung des Ausweises zu überprüfen und die für sie relevanten Attribute oder Eigenschaften des Ausweisinhabers dem Ausweis zu entnehmen. Beispiele sind die Identität, die Funktion oder auch nur die Eigenschaft, Mitglied der Stadtverwaltung, des Stadtrats oder eines Bezirksausschusses zu sein.
4. Die Nutzung des digitalen Ausweises sollte für die Beteiligten komfortabler sein als die Nutzung des analogen Ausweises oder zumindest andere Vorteile wie eine höhere Datensicherheit mit sich bringen.

Die dargestellten Eigenschaften der digitalen Ausweise entsprechen bekannten Anforderungen an digitale Identitäten. Digitale Identitäten sind die Grundlage einer durchgängigen Digitalisierung von Staat und Gesellschaft und daher zunehmend im Fokus der Betrachtung.

2. Digitale Identitäten

Auch die Stadtverwaltung beschäftigt sich seit der Einführung des elektronischen Personalausweises mit dem Thema digitale Identitäten. Wenn die Verwaltung eine digitale Transformation durchlaufen und ihre Verwaltungsleistungen digital und online zur Verfügung stellen soll, ist es in der Mehrzahl der Fälle eine notwendige Voraussetzung, dass sie die Bürger*innen und Organisationen, die diese Leistungen nutzen wollen, in digitaler Form identifiziert und authentifiziert. Nur nach sicherer Identifizierung der Antragsteller*innen kann die Verwaltung ihre Aufgabe im hoheitlichen Bereich rechtskonform erfüllen. Dieses Erfordernis zeigt sich bereits im OZG-Umfeld, wenn es dort auch in den wenigsten Fällen bisher umgesetzt wird, wird aber zu einer unumstößlichen Forderung, wenn alle Verwaltungsleistungen digital umgesetzt werden sollen.

Es ist für die LHM nicht zielführend, selbst als sog. Identity Provider für Bürger*innen / Organisationen zu fungieren, der für die Ausgabe sicherer digitaler Identitäten verantwortlich ist. Die LHM will sich vielmehr der digitalen Identitäten gängiger Identity Provider zur Identifikation der Bürger*innen und Organisationen bedienen, also lediglich als überprüfende Instanz fungieren. Im Sinne der oben dargestellten Eigenschaften muss sich die LHM bei diesem Ansatz darum kümmern, geeignete Identity Provider auszuwählen, die die Sicherheit der digitalen Identitäten im Sinne der Eigenschaften 1. und 2. aus Kapitel 1 erfüllen. Die LHM muss sich selbst in die Lage versetzen, die Aufgaben gemäß Nummer 3. aus Kapitel 1 auszuführen. Schließlich muss die LHM so flexibel sein, dass sie die digitalen Identitäten akzeptieren kann, die neben den Eigenschaften 1. und 2. aus Kapitel 1 auch eine komfortable Nutzung versprechen und damit die Eigenschaft 4. in Kapitel 1 aus Sicht der Nutzenden erfüllen. Denn nur diese Identitäten werden letztlich die Akzeptanz in der Gesellschaft finden. Die bisher fehlende Akzeptanz des neuen Personalausweises ist ausreichend Beleg dafür. Die Vorbereitungen, um sich dafür professionell aufzustellen, laufen seit geraumer Zeit, und versetzen die LHM heute schon in die Lage, die Bayern-ID als eine digitale Identität in den OZG-Formularen der LHM zu nutzen. Im Rahmen des gerade beschlossenen MPdZ-Projekts werden diese Aktivitäten weiter verstärkt, damit die LHM flexibel und zukunftssicher mit den digitalen Identitäten umgehen kann, die am Markt verfügbar sind und von den Bürger*innen und Unternehmen angenommen und eingesetzt werden.

Anders stellt sich die Situation dar, wenn es um die Nutzung von internen IT-Services der Verwaltung durch eigene Mitarbeitende oder auch andere Personen geht. Hier stellt sich dann die Frage, ob die LHM weiterhin nur die Rolle der überprüfenden Instanz einnimmt oder auch zum Herausgeber (Identity Provider) von digitalen Identitäten für diese Personengruppen wird und eigene digitale Ausweise für Mitarbeitende und andere Personen ausgibt.

3. Digitale Mitarbeiter*innenausweise

Ausweise für Mitarbeitende von Organisationen kombinieren heute oftmals die Möglichkeiten analoger und digitaler Ausweise. Einerseits unterstützen sie die Identifizierung und Authentifizierung des Inhabers auf Basis einer rein visuellen Überprüfung des Ausweises. Andererseits unterstützen sie auch die sichere Identifizierung und Authentifizierung des Inhabers gegen IT-Systeme, z. B. für den Login zum System selbst oder den Zugriff auf

andere digitale Ressourcen. Hierzu sind auf den Ausweisen kryptographische Mechanismen implementiert und Schlüssel hinterlegt, die eindeutig einer Identität über sogenannte (Public-Key-) Zertifikate zugeordnet sind. Diese Zertifikate werden über eigens dafür betriebene Zertifikats-Infrastrukturen ausgestellt und verwaltet. Es muss dann nur noch sicher gestellt werden, dass die Ausweise den berechtigten Inhaber*innen übergeben werden. Mit den angebotenen kryptographischen Fähigkeiten können die Ausweise üblicherweise auch für fortgeschrittene elektronische Signaturen eingesetzt werden.

Um diese Kombination analoger und digitaler Fähigkeiten anzubieten, werden diese Ausweise oftmals über Chipkarten als Formfaktoren realisiert. Diese ermöglichen neben den visuellen Merkmalen (Foto, Name, etc.) auf der Karte und den digitalen Identitätsfunktionen im Chip der Karte weitere Funktionen wie Bezahlen in Kantine oder physischer Zutritt zu Gelände oder Räumen (entweder über den Chip oder andere Komponenten der Karte). Erst durch diese Vielfalt von Möglichkeiten können die Kosten für das Beschaffen und das Management der Chipkarten und der dafür benötigten Infrastrukturen einem entsprechenden Nutzen gegenübergestellt werden. Es ist grundsätzlich möglich, die digitale Ausweisfunktionalität vollständig auf Smartphones zu realisieren, dies setzt aber voraus, dass die Smartphones über entsprechende sichere HW-Module und Fähigkeiten wie die Chipkarten verfügen und alle Mitarbeitende ein entsprechendes Smartphone besitzen. Unabhängig vom gewählten Formfaktor müssen die sogenannten Akzeptanzstellen, d. h. Instanzen, die die Ausweise überprüfen, um dem Prüfergebnis entsprechend Aktivitäten zu starten, ihre Aufgabe erfüllen können. Dies setzt voraus, dass sie derart in diese Zertifikats-Infrastrukturen integriert sind, dass sie der Infrastruktur vertrauen und die zur Prüfung nötigen Protokolle und Vorgehensweisen der Infrastruktur ebenfalls beherrschen. D. h., sobald diese Ausweise auch außerhalb der eigenen Organisation eingesetzt werden sollen, müssen die Akzeptanzstellen außerhalb der Organisation der Infrastruktur der Organisation vertrauen und über entsprechende Fähigkeiten verfügen. Dies ist ein bekanntes und für eine Organisation wie die LHM nur schwer zu lösendes Problem.

Da die LHM derzeit nur analoge Ausweise ausgibt, hat sich das RIT mit der Frage von Mitarbeiter*innenausweisen beschäftigt und die verschiedenen Möglichkeiten analysiert. Im Ergebnis wird die oben beschriebene Kombination aus analogen und digitalen Fähigkeiten aus Kostengründen nicht weiter verfolgt. Ebenfalls nicht weiter verfolgt wird derzeit die Möglichkeit, Smartphones als Träger der digitalen Identitäten einzusetzen, da dies wie oben beschrieben ebenfalls zu hohen Kosten führen würde. Der sichere Zugang zu IT-Systemen kann kostengünstiger realisiert werden. Dazu verfolgt die LHM den Weg, über sog. FIDO2 Security-Keys den Mitarbeitenden sichere Token an die Hand zu geben, mit denen sie den sicheren Zugriff auf IT-Systeme erhalten können und auch fortgeschrittene elektronische Signaturen ausstellen können. Diese Lösung ist benutzerfreundlich und macht die Digitale Identität eines Mitarbeitendem mit einem virtuellen Ausweis vergleichbar. Zudem können mit diesen FIDO2 Keys die derzeit im Einsatz befindlichen RSA-Token für den Fernzugriff abgelöst werden, wodurch sich eine Kostenreduktion beim Fernzugriff erreichen lässt. Diese Formfaktoren erlauben aber kein Aufbringen eines Merkmals für eine visuelle Prüfung. Die LHM beschreitet also den Weg, weiterhin analoge Dienstausweise für die rein visuelle Überprüfung zu nutzen und FIDO2 Security Keys für den Zugang zu IT-Systemen an die Mitarbeitenden auszugeben, die dann auch für elektronische Signaturen genutzt werden können.

Es ist möglich, diese Vorgehensweise auch auf Stadträte und BA-Mitglieder auszudehnen, wenn sie Zugriff auf interne IT-Systeme benötigen.

Da die Verwendung des FIDO2-Standards auch in anderen Internet-Bereichen zunimmt, können die den Mitarbeitenden ausgehändigten Keys auch zunehmend im privaten Um-

feld für einen sicheren Zugang zu Internet-Ressourcen und natürlich auch auf privaten Endgeräten genutzt werden.

4. QR-code basierte digitale Ausweise

Der in der Antragsbegründung angeführte Vergleich mit Impfausweisen legt allerdings nahe, dass die Antragsteller*innen einen deutlich einfacheren Ausweistyp hinsichtlich Identifizierung im Sinn haben als diejenigen, die in Kapitel 3 diskutiert wurden. Als Beispiel werden QR-Code-basierte Ausweise wie der Impfausweis genannt. Derartige Ausweise haben im Vergleich zu den FIDO2 Token ein deutlich niedrigeres Sicherheitsniveau sowohl im Hinblick auf die Fälschungssicherheit als auch im Hinblick auf die Inhaber-Identifikation. Ihr Einsatz setzt voraus, dass alle vorgesehenen Akzeptanzstellen in ein gemeinsames Ökosystem integriert sind und über entsprechende Prüffunktionalität, z. B. in Form einer geeigneten App verfügen. Angesichts der dargestellten Funktionalität der verfolgten Lösung für Mitarbeiter*innenausweise stellt sich die Frage nach dem Zweck eines derartigen zusätzlichen Ausweises innerhalb der LHM. Er würde ausschließlich zur visuellen Überprüfung der Identität dienen, um z. B. physischen Zugang zu erhalten. Zur Umsetzung dieser Lösung wären aber nicht nur Aufwände für die Ausweise selbst, sondern auch für die Ausstattung der Akzeptanzstellen mit Prüfmechanismen wie entsprechenden Apps nötig. Nur in diesem Fall wäre der digitale Ausweis dem analogen überlegen hinsichtlich Nutzerfreundlichkeit und Sicherheit. Außerhalb der LHM wäre der digitale Ausweis nur einsetzbar, wenn auch die dortigen Akzeptanzstellen über die entsprechenden Mechanismen verfügen würden. Es gibt aktuell keinen Ansatz, wie dies geschehen soll, da entsprechende Ökosysteme, die für die LHM offen und geeignet sind, derzeit nicht bekannt sind. Zudem muss darauf hingewiesen werden, dass für eine wirksame Kontrolle des Ausweises hier eine zusätzliche Identitätsprüfung, z. B. durch Personalausweis mit Lichtbild oder dem analogen Ausweis der LHM, erfolgen müsste (analog zur korrekten Kontrolle des Impfstatus), wodurch die Nutzerfreundlichkeit deutlich beeinträchtigt würde und ein Vorteil gegenüber dem analogen Ausweis nur schwer darstellbar ist.

5. Fazit

Die LHM verfolgt den oben dargestellten Ansatz über FIDO2 Security-Keys, um die Mitarbeitenden mit digitalen Token oder Ausweisen auszustatten, über die Zugriffe auf die IT-Systeme der LHM sicher und kryptographisch basiert möglich sind. Diese Token können auch Stadträten oder BA-Mitgliedern ausgehändigt werden, wenn sie den Zugriff auf interne IT-Systeme benötigen. Aus den in Kapitel 4 dargestellten Gründen ist der im Antrag geforderte digitale Ausweis als zusätzliche Lösung nicht sinnvoll umsetzbar und realisierbar. Kosten und Nutzen stehen in keinem sinnvollen Verhältnis. Aus diesem Grund wird weiterhin der eingeschlagene Weg verfolgt, mittels FIDO2 Security-Keys einen sicheren und nutzerfreundlichen Zugang zur IT-Infrastruktur anzubieten und für die rein visuelle Überprüfung von Identität und Funktion weiterhin den analogen Dienstausweis zu verwenden.

Der Stadtratsantrag 14-20 / A 04855 ist auf Basis der geschilderten Faktenlage geschäftsordnungsmäßig erledigt.

6. Beteiligungen/ Stellungnahmen der Referate

Die Beschlussvorlage wurde dem Direktorium (DIR), dem Personal- und Organisationsreferat (POR), der Gleichstellungsstelle für Frauen (GSt) und dem Gesamtpersonalrat (GPR) im Rahmen der verwaltungsinternen Abstimmung zur Stellungnahme zugeleitet.

DIR, POR, GSt und GPR stimmen der Beschlussvorlage in ihren Stellungnahmen zu. Der GPR weist in seiner Stellungnahme zusätzlich darauf hin, dass er neben der Diskussion um Ausweise eine schnellstmögliche Ausstattung aller Beschäftigten mit Smartphones für richtig und sinnvoll erachtet. Die Stellungnahmen sind der Beschlussvorlage als Anlagen beigefügt.

Korreferentin (RIT) und Verwaltungsbeirat (RIT-I)

Die Korreferentin des IT-Referats, Frau Stadträtin Sabine Bär, und der zuständige Verwaltungsbeirat von RIT-I, Herr Stadtrat Lars Mentrup, haben einen Abdruck der Sitzungsvorlage erhalten.

Verwaltungsbeirätin (it@M)

Die Verwaltungsbeirätin von it@M, Frau Stadträtin Judith Greif, hat einen Abdruck der Sitzungsvorlage erhalten.

II. Antrag des Referenten

1. Der Stadtrat nimmt die Ausführungen zur Kenntnis.
2. Eine Umsetzung des im Antrag geforderten digitalen Ausweises für Stadträt*innen, BA-Mitglieder und Mitarbeitende erfolgt nicht.
3. Mit diesem Beschluss wird der Stadtratsantrag Antrag Nr. 20-26 / A 01952 der Stadtratsfraktion CSU „Digitaler Ausweis“ geschäftsordnungsmäßig erledigt.
4. Der Beschluss unterliegt nicht der Beschlussvollzugskontrolle.

III. Beschluss

nach Antrag.

Über den Beratungsgegenstand wird durch die Vollversammlung des Stadtrates endgültig beschlossen.

Der Stadtrat der Landeshauptstadt München

Der / Die Vorsitzende

Ober-/Bürgermeister/-in
ea. Stadtrat / ea. Stadträtin

Der Referent

Thomas Bönig
Berufsm. Stadtrat

IV. Abdruck von I. mit III.
über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt

z. K.

V. Wv. - RIT-Beschlusswesen