

München Portal der Zukunft – Bürger*innen-ID (Kurzfassung)

1 Ausgangslage und Perspektive:

Digitale Identitäten (IDs) werden heute bereits von Bürger*innen in einer Vielzahl verschiedener Kontexte verwendet. Die Bürger*innen besitzen eine **Vielzahl von Benutzerkonten** aus ihrem privaten und beruflichen Umfeld, zu denen jeweils Stammdaten gehören. Wenn sich Bürger*innen mit diesen Konten beim Stadtportal anmelden, dann muss entschieden werden, ob und wie die damit verbundenen Stammdaten im Kontext der LHM verwendet werden.

Für die Zuordnung der unterschiedlichen der digitalen Identitäten zu **Vertrauensniveaus**¹ - gibt es Standards wie z. B. eIDAS Verordnung, Richtlinien vom BSI und NIST. Aktuell gibt es Bemühungen, alle Leistungen aus dem OZG den Vertrauensniveaus zuzuordnen.



Abbildung 1: Ausgangssituation digitale Identitäten bei Bürger*innen

2 Handlungsfelder

Aus der Ausgangslage und den Perspektiven leiten sich für die Gestaltung der Bürger*innen-ID zahlreiche Handlungsfelder ab, verteilt auf die Bereiche fachliche, technische und übergreifende Handlungsfelder.

Die fachlichen Themenfelder werden im Folgenden kurz skizziert:

- **Schutzbedarfe und Vertrauensniveaus:** Datensicherheit und Datenschutz sind zentrale Leistungsversprechen der LHM gegenüber ihren Bürger*innen sowie den Partner*innen aus der Wirtschaft. Hier darf es keine Missstände und Risiken geben, die das Vertrauen in die Fähigkeiten

¹ Abhängig von der Art der Transaktion und den dabei erforderlichen Daten wird der Schutzbedarf und damit die Anforderungen an die Stärke des digitalen Identifizierungsmechanismus bestimmt, die EU-Verordnung eIDAS unterscheidet drei Vertrauensniveaus.

der Stadtverwaltung beeinträchtigen. Mit zunehmender Digitalisierung, Open Data Initiativen und Plattformen zur Partizipation und Vernetzung steigt das Volumen an Daten und die Kontakt- und damit auch die Angriffspunkte wachsen an. Die verwalteten Informationen und technischen Ressourcen auf denen die Daten gespeichert und verarbeitet werden, müssen identifiziert, nach Schutzbedarf und Vertrauensniveaus klassifiziert und entsprechend abgesichert werden.

- **Identity Provider (IdP):** Bürger*innen, die sich in der digitalen Welt bewegen, nutzen eine Vielzahl elektronischer Identitäten von unterschiedlichen Anbieter*innen. Um es den Kund*innen leicht zu machen, könnten diese privatwirtschaftlichen IDs auch für einen Teil der Angebote und Leistungen aus dem Stadtkonzern genutzt werden. Für Verwaltungsleistungen sind aber vertrauenswürdige IDs erforderlich. D. h. jede Lösung in diesem Bereich muss verschiedenen ID Provider integrieren, deren Vertrauensniveau kennen und überwachen und die passende Auswahl der Identität für den jeweiligen Service sicherstellen.
- **Citizen & Consumer Identity and Access Management (C2-IAM):** Zu betrachten sind bei der Konzeption einer geeigneten „Sicherheitsarchitektur“ die Orchestrierung von Identitäten, die „Identitätsprovider“ selber und die „Schutzbedarfe und Vertrauensniveaus“ der Bürger*innen ID. Das C2-IAM Handlungsfeld fokussiert hierbei auf die technische Umsetzung der Orchestrierungsschicht, insbesondere in den Dimensionen Identity Management², Access Management, Verzeichnisdienste und Integration. Um dem übergreifenden und vor allem nach außen in Richtung Smart City gerichteten Kontext Rechnung zu tragen, wurde das Präfix „Citizen & Consumer“ – gegenüber dem klassischen IAM - ergänzt. Daraus ergeben sich neue Anforderungen, die klassische IAM Systeme typischerweise nicht abdecken. Hierzu gehören z. B. die Orchestrierung von unterschiedlichen IdPs, die Unterstützung diverser Protokolle (bspw. SAML, OIDC, OAuth), die technische Zusammenführung unterschiedlicher Profile (bspw. Login mit Google, Login mit BayernID), die Unterstützung unterschiedlicher Zugriffsmechanismen (bspw. rollenbasiert vs. attributbasiert) und die hohe Verfügbarkeit und Skalierbarkeit, wenn das C2-IAM System als zentrales System etabliert wird.

Zielbild und Empfehlungen:

Der Markt für digitale Identitäten und deren Provider befindet sich in vielen Bereichen noch im Aufbau. Für die LHM geht es darum die relevante Identity Provider zu identifizieren, ihre Anwendbarkeit im jeweiligen Anwendungsbereich passend zur Vertrauensstufe zu beurteilen und geeignete auszuwählen. Aktuell sind die BayernID für den hoheitlichen Bereich und der M-Login für den übrigen Bereich ausgewählt bzw. vorgegeben. Die Verbreitung und Akzeptanz der BayernID ist bei den Bürger*innen bislang sehr gering, sie ist allerdings für diverse Online-Dienste die einzig akzeptierte ID. Die Verbreitung des M-Login wird von den Stadtwerken München im Stadtgebiet stark gefördert. Social Media Logins werden momentan nicht von der LHM unterstützt.

² Identity Management bezeichnet die Verwaltung von Benutzer*innenkonten, Access Management die Verwaltung von Zugriffsrechten der Benutzer*innen auf Anwendungen und Ressourcen (z. B. Drucker, Datenablage etc.). Identity und Access Management (IAM) verbindet beide Dimensionen.

Es gibt im Kontext Bürger*innen-ID vier zentrale Handlungsstränge, um aus digitalen Identitäten, die Bürger*innen auch ohne Zutun der Landeshauptstadt bereits mehrfach besitzen (Google, Apple, Facebook, Amazon, Instagram, Online Banking, Yes.com, Verimi, BayernID, BundesID, Elster ID, M-Login, Muenchen Ticket, ...) eine „Bürger*innen-ID“ zu erstellen, die weniger auf die Menge („ist es genau eine ID“) als vielmehr auf das „was kann ich damit machen“ fokussiert ist.

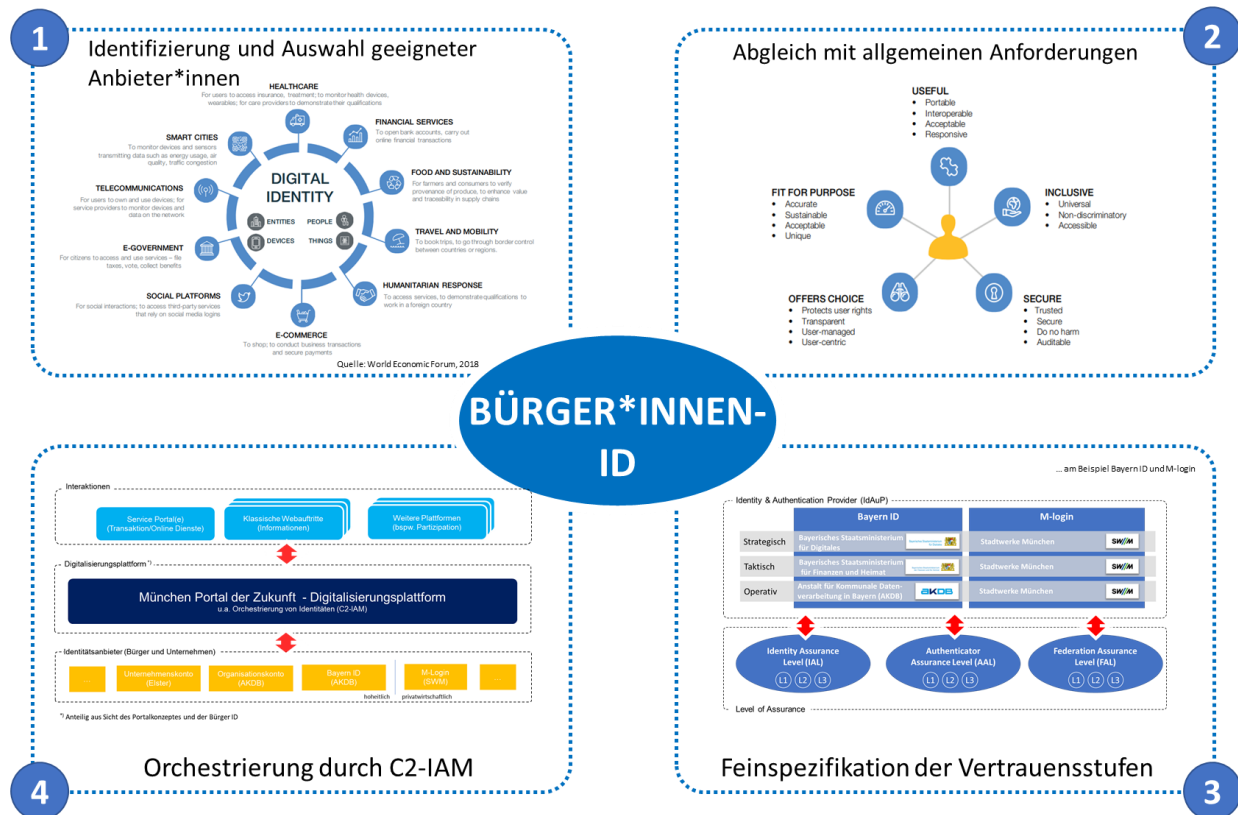


Abbildung 2: Zielbild und Handlungsstränge der Bürger*innen-ID

Ausdrücklich nicht empfohlen ist der Aufbau einer neuen, eigenen Bürger*innen-ID (also die LHM als eigener Identity Provider), mit folgender Begründung:

- Es gibt bereits mehr als genug professionelle Anbieter*innen auf dem Markt, die sinnvoll eingebunden werden können (bspw. Yes.com, Verimi, IDnow, NetID, ID4me, ...). Warum also selbst machen?
- Der Aufwand in Form von Zeit und Kosten steht unverhältnismäßig zum Ergebnis (eIDAS Compliance, BSI, ...). Selbst wenn diese neue ID technisch brillant wäre und alle Compliance Vorschriften erfüllt, müsste sie sich dennoch dauerhaft im Markt durchsetzen, um langfristig erfolgreich zu sein. Das setzt die Akzeptanz der Nutzer*innen voraus. Mit diesem Thema kämpfen auch Verimi & Co und nehmen dazu aber Millionen-Beträge für Marketing und Lobby-Arbeit in die Hand.