Symbolbild: Onlinezugangsgesetz (OZG) einfach & treffsicher umsetzen

07.09.2020 09:00 CEST

Onlinezugangsgesetz - OZG – einfach & treffsicher umsetzen

Wird die Digitalisierung der Verwaltungen durch den deutschen Föderalismus behindert? Ein Beitrag von Jürgen Vogler, Geschäftsführer der procilon GROUP GmbH

Im Jahr 2018 veröffentlichte das Handelsblatt ein „EU-Ranking für den Bereich digitale öffentliche Dienste“. Deutschland fand sich abgeschlagen auf Platz 21 und wer Estland auf Platz 1 vermutete, liegt richtig. Begründet wird dies gern mit der Formulierung „die sind ja auch zentral organisiert und haben keine föderale Struktur“. Aber ist eine föderale Struktur wirklich ein Hinderungsgrund? Meine klare Antwort auf dies Frage heißt: NEIN!

Eine solch klare Aussage will ich auch gern begründen. Dazu sollten zwei grundlegende Aspekte betrachtet werden.

Als Unternehmen der IT-Sicherheitsbranche beurteilen wir Projekte nicht nur aus technischer, sondern auch aus organisatorischer Perspektive. Ich will mit den organisatorischen Aspekten beginnen. Insbesondere für den Bereich der öffentlichen Verwaltung finden wir hierfür eine Reihe von Vorschriften, Verordnungen und Gesetzen, die den Spielraum abstecken. Allen voran das Online-Zugangs-Gesetz. Hier wurde zum Glück technikneutral die Anforderung definiert, dass Bürger alle angebotenen E-Government-Leistungen mit nur einer elektronischen Identität nutzen können sollen. Dies hat in der ersten Konsequenz eine, nennen wir es ruhig, „Estlandisierungswelle“ ausgelöst, verbunden mit allen Hindernissen, die sich dann im föderalen Verwaltungsgefüge auftun können. Der Gedanke, dass der Nutzer -also der Bürger - dabei nicht immer die oberste Priorität hatte, drängt sich geradezu auf. Auch lassen sich die vielen E-Government-Anwendungen, Registrierungen oder vorhandene Bürgerkonten auf den ersten Blick organisatorisch nur schwer harmonisieren. Und nicht zuletzt trifft man hier auch auf monetäre Interessen einzelner Hersteller und Anbieter. Mit dem neuen Bundes CIO hat sich hier einiges bewegt und das gibt Hoffnung.

Damit komme ich zu den technischen Aspekten, denn daraus leitet sich diese Hoffnung ab.

Föderale Strukturen sind in der Informationstechnik nichts Unbekanntes. Wer sich einmal intensiver mit den Themen Identity-Access-Management oder Trusted-Domain-Konzepten beschäftigt hat, wird mir zustimmen. Wie die Begriffe schon vermuten lassen, liegt die Lösung in der Verbindung von Identität und Vertrauen. Kurz gesagt benötigt ein Nutzer eine vertrauenswürdige Identität, um vertrauenswürdige E-Government-Dienste nutzen zu können.

Insbesondere vor dem Hintergrund des Online-Zugangs-Gesetzes kommt es nun darauf an, all diese verschiedenen Identitäten über ein intelligentes Identity- & Access-Management im Sinne eines Identitätsbrokers zu verbinden. Der Bedarf für solche Lösungen wird durch den Wegfall des sogenannten Portalverbundes noch verstärkt.

Verständlicherweise haben öffentliche Verwaltungen von der Kommune bis zur Bundesbehörde ein großes Interesse an bestätigten Bürger-Identitäten. Nur mit diesen können verbindliche Interaktionen, wie z. B. das Ausfüllen von Formularen vollständig medienbruchfrei abgebildet werden. Wird in einen solchen Verwaltungsprozess die digitale Unterschriftsmöglichkeit für den Bürger ergänzt, ist das Ziel einer Digitalen Transformation tatsächlich erreicht. Solch ein Szenario geht über die allgemeine Forderung des OZG, der Bürger muss auf alles Zugriff haben‘ weit hinaus. Denn erst mit der Kombination von universellem Zugriff UND digitaler Unterschrift entsteht

der oft zitierte Mehrwert und vor allen Dingen ein erkennbarer Nutzen, der deutlich die Akzeptanz erhöht.

Vom Design solcher Lösungen kehren wir kurz zum organisatorischen Rahmen zurück, verlassen aber den nationalen Raum und wenden uns der eIDAS-Verordnung der Europäischen Kommission zu. Irrtümlich wird oft davon geredet, dass diese die Verwendung elektronischer Signaturen regelt. Richtig betrachtet, regelt sie aber primär den Umgang mit elektronischen Identitäten und damit letztendlich auch, was man damit machen kann. Hier erfolgt eine Einstufung einer elektronischen Identität anhand eines Vertrauensniveaus in "niedrig", "substanziell" und "hoch". Beschrieben wird weiterhin, dass ein elektronisches Identifizierungsmittel nur dann als "substanziell" oder "hoch" anerkannt wird, wenn der Mitgliedstaat dieses im Rahmen eines in der eIDAS-Verordnung festgelegten Verfahrens auf dem entsprechenden Vertrauensniveau notifiziert hat. Dies kann sinngemäß auch auf den Anwendungsbereich des OZG übernommen werden. Für Verwaltungen bietet sich damit die Chance, die Generierung bzw. Anerkennung von bestätigten Bürger-Identitäten zu regeln und die jeweiligen Anwendungsfälle so zu gestalten, dass eine wirklich durchgängige, also medienbruchfreie, Transformation stattfindet.

Der kritische Nutzer will sich aber nicht immer wieder an einem neuen System mit all seinen Daten registrieren müssen. Denn sowohl im dienstlichen als auch im privaten Umfeld haben wir alle schon eine Vielzahl von elektronischen Identitäten. Eine Registrierung wird sich nicht vollständig verhindern lassen, aber sie kann deutlich vereinfacht werden. Dafür wird ein neuer Mitspieler benötigt: Der Identitätsprovider.

Hier etablieren sich aktuell einige Unternehmen, die vertrauenswürdige Identitäten als Geschäftsmodell erkannt haben. Exemplarisch seien hier Anbieter wie Verimi oder Yes genannt. Auf der anderen Seite verfügen gerade öffentliche Einrichtungen wie Kommunen und Krankenkassen aber auch Banken, Versicherungen, Verbände und Kommunen über ein Potential, das genutzt werden kann.

Ein initialer Registrierungsprozess erfolgt meist durch Selbst-Registrierung. Interessant wird es für den Bürger dann, wenn er im Rahmen einer automatisierten Registrierung die Möglichkeit erhält, bereits bestätigte vertrauenswürdige Identität mitzubringen. Hierbei gilt, je besser das Niveau der elektronischen Identität, desto mehr nähern wir uns den eIDAS-Kriterien an. Das Wirkprinzip besteht darin, die für die Nutzung eines OZG-Dienstes notwendige Registrierung mit einer vertrauenswürdigen Identität eines Identitätsproviders zu verknüpften. Wie oben geschildert, spricht nichts dagegen, dass, neben kommerziellen Anbietern, auch Kommunen diese Rolle übernehmen können. Im Sinne des OZG muss jetzt nur noch dafür gesorgt werden, dass sich im Wirkungsbereich des OZG alle Beteiligten in Sachen elektronischer Bürger-Identität vertrauen. Hierfür kommt ein sogenannter Identitätsbroker zum Einsatz, der alle vertrauenswürdigen

Identitätsprovider kennt und alle notwendigen Nutzerinformationen entsprechend einer Rechte- und Rollendefinition an Fachanwendungen oder Web-Portale weitergibt. Damit erhalten alle Verwaltungen die Möglichkeit, digitale Verwaltungsprozesse auch weiterhin mit ‚ihren' Anwendungen individuell zu gestalten. Für die Hersteller von Fachanwendungen entsteht lediglich der Aufwand, die Zugriffsmechanismen ihrer Web-Anwendungen oder Formular-Server auf die Integrationsmöglichkeiten zu einem normierten Identity- & Access-Management zu überprüfen und ggf. anzupassen. Ist dies hinreichend gegeben eröffnen sich neben dem reinen Zugriff auf Dienste und Leistungen eine Reihe weiterer Möglichkeiten, die von der einfachen elektronischen Unterschrift durch Fernsignatur bis hin zum gesicherten elektronischen 'Rückkanal' von der Verwaltung zum Bürger reichen.

Wer jetzt noch einen Beweis braucht, wie solche Konzepte in der Praxis sicher und zuverlässig umgesetzt sind, möge sich den elektronischen Rechtsverkehr ansehen. Hier wird mit SAFE (Secure Access to Federated e-Justic/E-Government) schon seit Jahren die Verwendung sicherer elektronischer Identitäten in einem föderalen Umfeld praktiziert. Der große Vorteil von SAFE besteht auf der einen Seite aus einer offenen Standardisierung und auf der anderen Seite der Möglichkeit, durch verteiltes Identity Management eine Vertrauensstellung zwischen Identitätsprovidern herzustellen. Praktiziert wird dies schon heute für Justizbehörden, Notare, Rechtsanwälte, Bundes-, Landes- und Kommunalverwaltungen, sowie Körperschaften des öffentlichen Rechts.

Mit anderen Worten, hat ein Nutzer einmal eine bestätigte elektronische Identität in ‚seiner' SAFE-Domain und wird diese von anderen SAFE-Domains akzeptiert, braucht er sich dort nicht neu registrieren und kann alle Dienste nutzen, die seiner Rolle entsprechen. Nach diesem Prinzip können zum Beispiel Rechtsanwälte und Notare mit ihrer elektronischen (SAFE-) Identität nicht nur am elektronischen Rechtsverkehr teilnehmen und Nachrichten an Gerichte schicken, sondern erhalten damit beispielsweise Zugriff auf das Zentrale Vorsorgeregister (Online-Dienst) der Bundesnotarkammer. Die Infrastruktur dafür ist vorhanden. Zu klären wäre nur, wie sich weitere Identitäts-Provider in diese Infrastruktur integrieren. Und damit schließt sich der Kreis, denn dies ist nicht nur eine technische Aufgabe. Hierfür sind wieder organisatorische Aspekte zu klären. Da aber föderale Verwaltungsstrukturen auf eine passgenaue Technik treffen, schöpfe ich genau daraus meine Hoffnung.

Die Unternehmen der procilon Gruppe haben sich seit fast 20 Jahren auf die Entwicklung kryptologischer Software spezialisiert. procilon-Lösungen sichern und verwalten digitale Identitäten, sorgen für vertrauenswürdige Kommunikation und schützen die Integrität gespeicherter Daten. Bereits

mehr als 1500 Unternehmen und Organisationen haben Maßnahmen zum präventiven Schutz sensiblen Daten mit procilon Unterstützung ergriffen.

Die Software-Technologie der procilon erfüllt sowohl nationale als auch internationalen Standards und Vorgaben. Einige Produkte wurden u. a. nach Common Criteria EAL 4+ AVA VAN.5 (Angriffspotential hoch) evaluiert und zertifiziert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erteilte eine Zertifizierung für die Lösung zur Langzeitarchivierung qualifiziert signierter Dokumente. Das einzigartige Produktspektrum reicht von einfacher Dateiverschlüsselung im Browser über Signaturanwendungen, Identity- & Access-Management bis hin zu kompletten Infrastrukturen für Vertrauensdiensteanbieter nach EU-eIDAS-Verordnung. Vielfältige sichere Services aus der Cloud runden das Portfolio ab.

Kontaktpersonen

Andreas Liefeith
Pressekontakt
Leiter Marketing & Unternehmenskommunikation
presse@procilon.de
034298 4878 10

Jürgen Vogler
Geschäftsführer
anfrage@procilon.de