Web Sicherheit

# Identity Federation der nächsten Generation: E-Government im Kanton Aargau

Juni 14, 2016 12:41pm

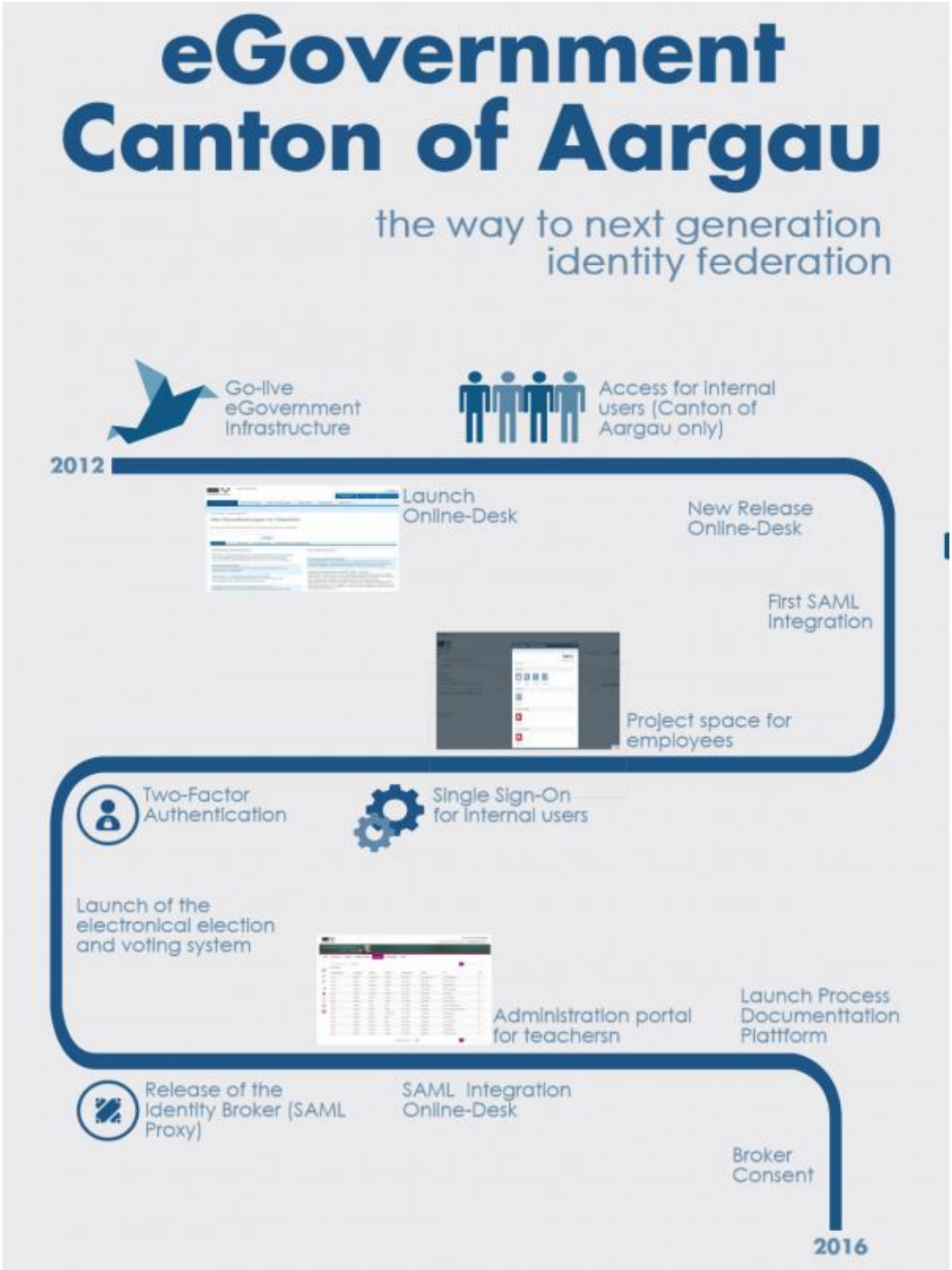
Der Kanton Aargau setzt auf bewährte Standards im E-Government. Mit der konsequenten Verfolgung einer serviceorientierten mehrschichtigen Architektur ermöglicht der Kanton es seinen Bürgerinnen und Bürgern, Verwaltungsmitarbeitenden, Institutionen und Drittparteien elektronische Verwaltungsdienstleistungen via einem zentralen Online-Portal zu nutzen. Die aargauische E-Government-Architektur wurde, einmalig in ihrer Flexibilität und ihren modularen Ausbaumöglichkeiten, von verschiedenen Gremien mehrfach ausgezeichnet. Unter anderem mit dem 3. Platz als innovativstes E-Governmentprojekt 2014 beim internationalen eGovernment-Wettbewerb . Seither baut der Kanton Aargau seine Vorreiterrolle Schritt für Schritt weiter aus – auch über die eigenen Kantonsgrenzen und föderalen Strutkuren hinweg.

## E-Government Infrastruktur des Kantons Aargau

### Grosse Bauvorhaben benötigen sichere Fundamente

Mit dem Launch eines Online-Schalters für elektronische Verwaltungsdienstleistungen lancierte der Kanton Aargau 2012 sein E-Government Angebot in Form eines zentralen Portals. Dass sich der Kanton Aargau auf dem richtigen Weg befindet, bestätigt Gartner 2015 in einer Studie, die den Portalansatz als attraktivste Variante betrachtet, um Bürgern Verwaltungsdienstleistungen via Internet zugänglich zu machen. Dabei sehen die Gartner-Analysten die Security-Infrastruktur und insbesondere die Wahl der richtigen Online-Credentials als kritische Erfolgsfaktoren für eine erfolgreiche Realisierung von E-Government Portalen. Laut Gartner müssen Credentials für den Zugang zu E-Government Services einfach erhältlich, leicht verwendbar und ausreichend sicher sein.

Der Online-Schalter des Kantons Aargau basiert auf einem breit abgestützten, stabilen Fundament einer 7-Schicht Architektur, die in allen Schichten auf eine modulare Bauweise setzt. Jeder einzelne Layer der 7-Schichten Architektur ist wichtig und hilfreich – auch die komplexe IT-Sicherheit. Der Kanton Aargau betrachtet den Security Layer nicht als notwendiges Übel, sondern wertet diesen als zentralen Bestandteil für den erfolgreichen Ausbau seiner Online Services.




*eGovernment Kanton Aargau: Der Weg zu Identity Federation der nächsten Generation*

### Security Layer als Brücke für E-Government

Sicherheit spielte von Beginn an eine tragende Rolle in der aargauischen E-Government Infrastruktur. Viele der in den letzten Jahren erreichten Meilensteine und gefeierten Erfolge von elektronischen Dienstleistungen hängen direkt mit der hohen Flexibilität im Security Layer zusammen:

Nebst einer Web Application Firewall, die die Verfügbarkeit der Online-Angebote sicherstellt und die Integrität von Anwendungen und Transaktionsdaten gewährleistet, ist vor allem das Access Management ein eminent wichtiger Bestandteil der gesamten Architektur. Angesiedelt im Security Layer mit dem USP Secure Entry Server® übernimmt es zentral die Authentisierung für alle internen und externen Zugriffe auf den Online-Schalter mit den dahinterliegenden Fachapplikationen.

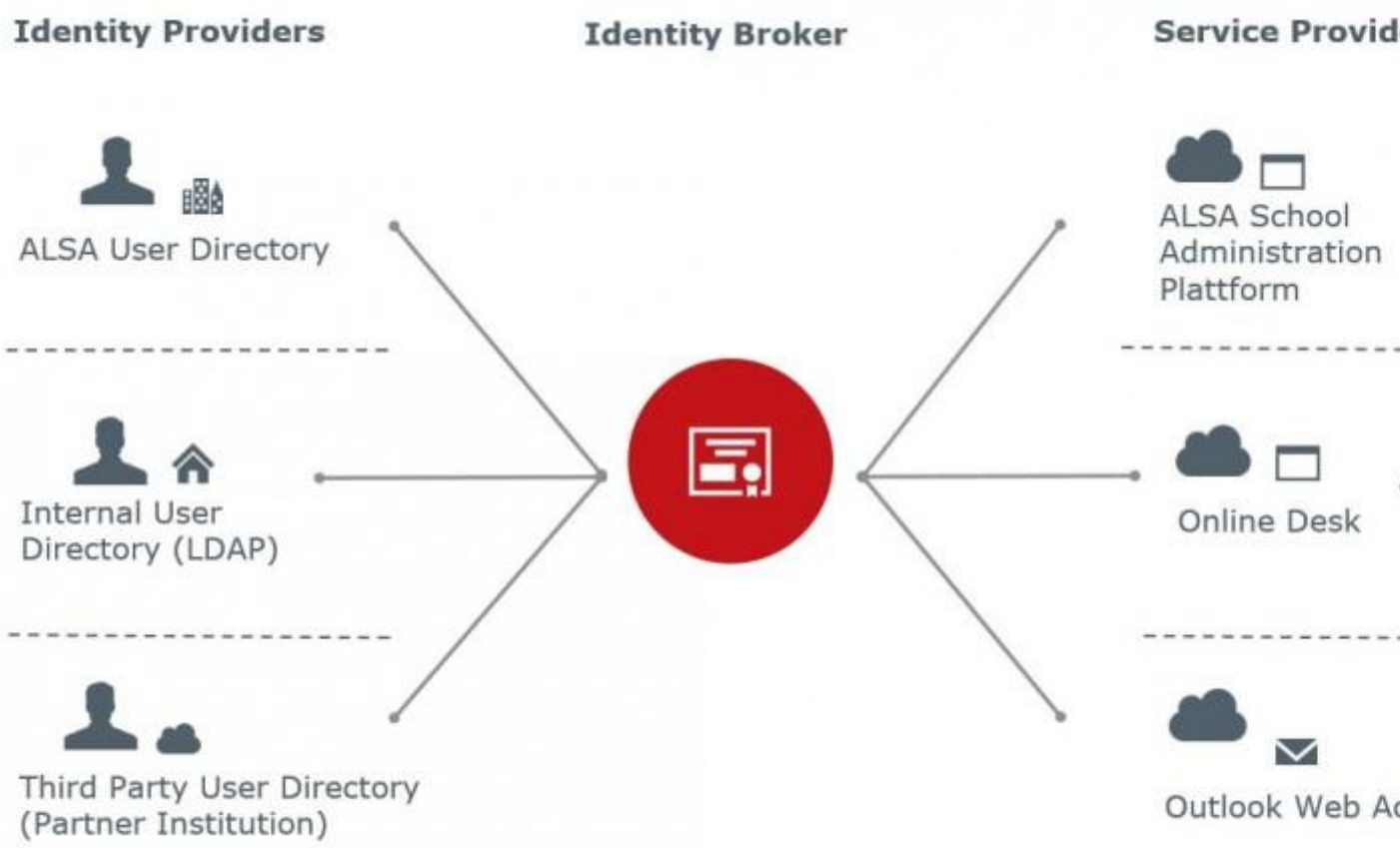
Im Zuge der weiteren Entwicklung wurden für interne und externe Mitarbeitende nutzbare Services wie Projekträume, Dokumenten-Ablagen und Fachprozesse wie z.B. der elektronische Einbürgerungsprozess, der Lotteriebewilligungsprozess, etc. angebunden. Die Authentisierung der Mitarbeitenden erfolgt vom internen Arbeitsplatz aus via Kerberos. Für Zugriffe aus dem Internet ist ergänzend die Authentisierung via SMS mTAN (Multi-Faktor-Authentisierung) möglich.

## Cloud SSO & Federation entfesseln das E-Government Potential organisationsübergreifend

Mit der Integration des Schulportals ALSA betrat der Kanton Aargau Neuland, indem er erstmals einen externen Service in sein E-Government-Gefüge integrierte. Die Nutzer des Schulportals sollten dabei ihr bisheriges Login nutzen können. Zu diesem Zweck wurde mit dem neuen Service auch gleich ein neuer Identity Provider integriert.

### Identity Broker für das E-Government der nächsten Generation

Um das Potential im E-Government voll zu entfalten, entschied sich der Kanton Aargau für die Erweiterung der modularen Sicherheitsschicht um einen SAML Proxy. Der sogenannte «Identity Broker» von United Security Providers übernimmt als zentraler Hub die Koordination zwischen allen Identity Providers und allen Service Providers.




*Der Identity Broker übernimmt als zentraler Hub das Authentisierungs- und die Autorisierungsmanagement der Benutzer und ermöglicht domänen-übergreifenden Single Sign-On mit weitreichenden Möglichkeiten (z.B. Consent, Transformation, Concealment, Provisioning)*

Der Identity Broker erhöht die Flexibilität in zwei Richtungen:

- Neue Services können schnell und datenschutzkonform in das E-Government Angebot aufgenommen werden.
- Bei der Zusammenarbeit mit neuen Partnerinstitutionen werden die aargauischen Services einem neuen Benutzerkreis einfach zugänglich gemacht. Diese können dabei ihre vertrauten Login-Daten nutzen. Der neue Identity Provider wird einfach am Identity Broker integriert (Herstellung von Trust Beziehungen).

Der Identity Broker (SAML Proxy) übernimmt die Koordination zwischen allen Identity Providers und allen Service Providers und bietet eine ganze Palette an Funktionalitäten für eine feingranulare Justierung an Bedürfnisse punkto Authentisierung und punkto Datenschutz:

- Transformation: Der Identity Brokerfungiert als „Übersetzer“ zwischen Identity Provider und Service Provider. Erfolgt die Authentisierung an einem Service über einen externen Identity Provider, transformiert der Identity Broker die Identitätsattribute (z.B. E-Mail, Mail und email) in eine einheitliche Form.
- Verschleierung: Der Identity Broker kann Identitätsattribute von Benutzern gegenüber dem Service Provider verbergen (z.B. UserID verschleiern) oder die Benutzer bei Bedarf gegenüber dem Service komplett anonymisieren (Datenschutz).
- Consent: Der Identity Broker informiert den Nutzer, sobald gewisse Eigenschaften seiner Identität (Attribute) an den Service weitergegeben werden und holt bei ihm das Einverständnis zur Weitergabe seiner Daten ein.
- Provisionierung: Via einem externen Dienst können neue Benutzer im LDAP angelegt werden.

## Single Sign-On über alle Plattformen hinweg

Dank der zentralisierten Authentisierungskomponente erfolgt nach einer einmaligen erfolgreichen Anmeldung ein Single Sign-On (SSO) über alle zur Verfügung stehenden Portale hinweg, für die der Nutzer berechtigt ist. Dieser interne Cloud SSO erhöht die Benutzerfreundlichkeit markant und ist ein wichtiger Bestandteil für die Effizienz der Prozesse in der heterogenen Servicelandschaft.

## Dynamische Erhöhung der Qualitätsstufen in der Authentifizierung

Was würde passieren, wenn ein Benutzer innerhalb einer aktiven Session von einem Service mit einem niedrigen Trust-Level zu einem anderen Service wechseln will, der eine hohe Qualität in der Authentifizierung erfordert? Zum Beispiel, wenn ein Benutzer nur mit Username/Passwort angemeldet, weil er am Online-Schalter eine Lotteriebewilligung eingeholt hat und anschliessend – da er ja bereits angemeldet ist – noch auf seine Steuererklärung zugreifen möchte?

Der Verein eCH, der für die Schweiz Standards im E-Government definiert, stellt im Standard eCH0170 ein Qualitätsmodell für elektronische Identitäten vor. Der Standard definiert, dass für virtuelle Ausweise dasselbe gelten muss wie für physische Ausweise. Ein Ausweis muss bestimmten Anforderungen genügen, um eine dem Anwendungsszenario angepasste Qualität in der Identifikation seines Trägers zu erlauben. Der eCH0170 Standard misst der elektronischen Identifizierung eine herausragende Bedeutung zu und definiert vier Qualitätsstufen für die zuverlässige Identifikation von Benutzern in elektronischen Verwaltungsprozessen.

Der Kanton Aargau macht zu diesem Zweck laufend neue Authentisierungs- und Identifikationsmethoden bzw. Produkte als modulare Basis-Services innerhalb des E-Governments zugänglich. Der Nutzer soll in Zukunft innerhalb der in den Portalen angebotenen Services die Qualität der Authentisierung dynamisch erhöhen können und erhält danach Zugriff auf Services, die eine höhere Qualität für die Authentisierung verlangen.

## Meine Identität gehört mir! – Herausforderungen im Bereich Identifizierung

Die grösste Herausforderung bleibt die Identifikation der Benutzer für Services, die einen Zugang auf sensible Daten wie Personen oder Finanzdaten ermöglichen. Dazu ist, gemäss dem eCH0170 Standard, die höchste von vier Qualitätsstufen für die Identifizierung erforderlich. Dieses Vertraulichkeitsniveau kommt beim Zugriff auf einen Service, der ein Höchstmass an Vertraulichkeit verlangt, zum Tragen. Ein Nutzer sollte dafür mindestens einmal physisch identifiziert werden. Dazu braucht es geeignete Methoden. Die eingesetzten Authentisierungsmittel für den Zugriff auf solche Services müssen ebenfalls höchsten Qualitätsansprüchen genügen. Heute gibt es eine Vielzahl an Möglichkeiten, rechtlich verbindlich auf höchster Stufe steht allerdings nur die SuisseID zur Verfügung.

Das Bestreben des Kantons Aargau ist, mit seinen elektronischen Dienstleistungen auch in Zukunft möglichst nah bei der Bürgerin und dem Bürger sowie der Wirtschaft zu sein. Mit einfach zugänglichen Services will der Kanton Aargau den Nutzern des E-Government Angebots einen möglichst grossen Nutzen und hohen Komfort bieten. Dies immer in der Balance zwischen Anforderungen und gesetzlichen Rahmenbedingungen.

Durch die Ausweitung der Authentisierungsmöglichkeiten und der zuverlässigen Benutzeridentifizierung mittels elektronischen Ausweisen wird in naher Zukunft ein grenzenloser Cloud Single Sign-On über alle Portale hinweg möglich sein. Bedingung hierzu ist allerdings, dass die stark fragmentierte Identitätslandschaft zentralisiert oder dezentralisiert homologiert wird. Ein über alle föderalen Ebenen anwendbares Modell mit standardisierten Schnittstellen würde die Entwicklung beschleunigen.

## Details zum Autor

Marco Bürli

Leiter E-Gov-Projekte - Kanton Aargau