Protokoll

Protokoll Sitzung AG-IZ

Datum: 10.12.2018 , 10:00 – 16:00 Uhr
Ort: MA 14, 1220 Wien, Stadlauer Straße 56, Besprechungsraum Polaris

Teilnehmer:

Siehe Teilnehmerliste

Inhaltsübersicht

Inhalt

Top 1: Tagesordnung und Protokoll

Tagesordnung und letztes Protokoll

Vorgehen / Beschluss

Müller merkt zum letzten Protokoll an: TO 14 – PVP-roles – soll als typisches Attribut markiert werden. Wird als Anmerkung zum letzten Protokoll aufgenommen.

Ebenfalls besprochen das Dokument VKZ (Verbleib bei den Standarddaten). Das Dokument wurde aber bereits in die AG-IZ übernommen. Die VKZ Clearing Gruppe bleibt aber bestehen.

Top 2: Bericht SubAG Policy (Reif)

Bericht der letzten Sitzung Sub-AG Policy.

Vorgehen / Beschluss

Es hat keine Sub-AG Policy stattgefunden.

Top 3: Bericht SubAG PVP (Lenz)

Bericht der letzten Sitzung der Sub-AG PVP.

Vorgehen / Beschluss

Lenz ist verhindert, Hörbe berichtet.

Teilnehmerverwaltung der zentralen Dienste: Use-Cases bei Reorganisation von Organisation wurden besprochen (häufig beim Bund, auch bei Länder, Gemeinden).

Bzgl. Umbenennung: ist der Rechtsnachfolger des Teilnehmers, für alle anderen ist ein neuer Vertrag notwendig. Spezifikation wurde aktualisiert, Feedback erfolgt durch Pichler und Stradal.
Prototyp soll in provisorisch in Betrieb genommen werden.
Einwand Stradal: provisorischer Betrieb ist schlecht, es muss ein sicheren Betrieb hergestellt werden. Hörbe: Die Umsetzung soll durch den Magistrat Wien erfolgen.
Pichler: Organisatorische Dinge sollen noch beleuchtet werden.
In der Sub-AG werden Provisioning Schnittstellen abgestimmt.

Nächster Termin für Sub-AG PVP soll abgestimmt werden. Pesendorfer stimmt sich mit Lenz für Termin im Jänner ab.

Müller: Mitabstimmung der zusätzlichen Punkte, die unter Allfälliges eingebracht wurden: gvApplId: erlaubte Zeichen; Zeichensatz in der LDAP-Spezifikation hat sich geändert. (soll in der Sub-AG-PVP mitbedacht werden).

Vorgehen bei der PV-Version Änderung; z.B. Änderung des zentralen LDAP? Welche Auswirkungen gibt es? In welcher Version muss es befüllt werden?

Die PVV muss aktualisiert werden, die Nomenklatur muss der DSGVO angepasst werden (es gibt keine Dienstleister mehr), Strukturänderung, formale Anpassung. Anmerkung Pesendorfer: die PVV wird betreffend die DSGVO bereits in der AG-ReSi aktualisiert? Nächste Termin der AG-RESI ist der 12.12.2018 (aktuelle Version PVV 1.2.1).

In welcher Version muss die PAI befüllt werden?
Pesendorfer: Eingegeben werden kann nur der alte Zeichensatz;

Stradal: Zentrale Dienste
Bei Org-Änderungen ist es leichter mit Rechtsnachfolger (aus Datenschutzsicht);
Besser wären trotz allem neue Verträge.

Stmk: Provisioning: Hr. Gamauf (betreibt das Provisioning in der Stmk) ist zum Schluss gekommen, es als Erweiterungsidee in die LFRZ Standardportal Gruppe einzubringen und nicht wie ursprünglich angedacht selbst entwickelt werden.
Pichler: Anfang des Jahres LFRZ Standardportal LA geplant; Jänner 2019, sollte dort bis Mitte Jänner eingebracht werden.

TOP 4: Sicherheitsklassen (Wittmann)

Statusbericht aktueller Stand der SecClass-Dokumente.

Vorgehen / Beschluss

Es hat keine Sitzung stattgefunden. Zuletzt 8.10.2018: Entwurf Secclass 4.0 Dokument. Entwurfs-Dokument wird als Beilage zum Protokoll versendet. Im E-Mail soll enthalten sein, bis wann ein Feedback erwartet wird.

Offen ist System Principal SecClass 3 – Problem.
Pichler: Analog wie die Stammportale; Authentifikation mittels Zertifikat müsste ausreichen. Sicherheitsklasse hängt am Recht;

Regeln für die Berechtigung für Application-User sind zu definieren.
Stradal: es ist zu beschreiben, wie es zulässig ist.

TOP 5: Erstbefüllung PV-LDAP (Pesendorfer)

Status der Erstbefüllung des Portalverbund-LDAP

Vorgehen / Beschluss

Pesendorfer: BMI hat Daten der Organisationen letzte Woche zur Verfügung gestellt, Informationen zu den Portalen sollen diese Woche kommen.
Soll komplett bis Ende Jänner 2019 erledigt werden.

Stradal: Unklarheiten bei (Staatsbürgerschafts-)Verbänden (Staatsbürgerschafts- und Standesamtsverband). Wien hat keine neuen Organisationen/Informationen.

Pichler: Sobald ein aktueller Stand vorhanden ist, soll der über die LDAP Server zur Verfügung gestellt werden.
Stradal: Jede Organisation die vertreten sein soll, muss danach prüfen, ob die Daten korrekt sind bzw. Informationen ergänzt werden müssen.

TOP 6: Klarnamen in OU (Stradal)

Klarnamen für OU in "gerichtstauglicher Form" und allfällige Anpassung von LDAP- und PVP-Spezifikationen dazu.

Vorgehen / Beschluss

Die meisten Teilnehmer haben die OU umgesetzt, einige fehlen noch wie z.B. Das BM.F.
BM.F: Die Testinstanzen sind noch nicht angebunden, voraussichtlich ab Jänner 2019.

In PVP 1.9 funktioniert alles bis auf die Bundesdienststellen. Es ist nicht bekannt welche Dienststelle sendet (alle mit B100…). Der Name ist zu wenig sprechend.

ldpa.gv.at als Schema fürs OU-Attribut „Kurzbezeichnung“ – Änderungen sollen dort erfolgen (OU von gvOrganisation). Soll bei der nächsten Aktualisierung berücksichtigt werden - mit Beispielen für eine Kurzbezeichnung.
Oberösterreich sendet interne Kurzbezeichnungen, diese werden von OÖ sicher nicht geändert bzw. angepasst.

BMI: Ersucht um Begründung, warum es für diese und jene Organisationeinheiten nicht gemacht werden kann, diese sollte ausreichend für seinen Datenschutzbeauftragten sein.

Hörbe: Aufwand der zentral beim BM.I gemacht werden soll. Der Aufwand würde sich auf die Bundesländer vervielfachen und ist daher nicht zu rechtfertigen.

Fazit: AG-IZ empfiehlt eine Lösung an einer zentralen Stelle.

TOP 7: Beschluss PVP SMA (Reif)

Aktueller Status der aktuellen Version PV SMA 1.4
Beschluss des Dokumentes in der AG-IZ.

Das Dokument wird mit der TO versendet.

Vorgehen / Beschluss

Vorstellung erfolgte in der letzten AG-IZ. Es kamen keine Anregungen, daher soll heute der Beschluss erfolgen. Folgende Änderungen wurden vorgenommen
TLS 1. Von gelb auf rot
TLS 1.3 als neues grünes Protokoll
Richtlinien gelten nun auch für Stammportale, Identity- und Service-Provider; allerdings ohne verpflichtenden Scans
Gültigkeitsdatum wäre ab 10.6.2019.

(Stmk: Automatische Scans sollen in PV Grundschutz aufgenommen werden; siehe letztes Protokoll). Anwendungsportalbetreiber sollen rechtzeitig informiert werden, damit das Dokument rechtzeitig an Kunden ausgesendet werden kann.

Das Dokument wird hiermit beschlossen und an alle gesendet.

Klauser: Automatische TLS Scans sind in der AG-Leiterrunde noch nicht abgestimmt; daher kein statusupdate.

Reif: Aussendung vom Depositar mit dem neuen SMA?

Liste zu scannenden Portalen; Tool soll auch interne Portale aufrufen können.

TOP 8: Umstellung PV CA 2 BM.I (Wittmann)

Umstellung der Zertifikatinfrastruktur beim BM.I. Probleme und weitere Vorgehensweise, Auswirkungen auf die Teilnehmer.

Vorgehen / Beschluss

Wittmann ersucht um ausreichend Vorlaufzeit zur Umstellung!

Stadt Wien betreibt zusätzlich zum BM.I eine CA.

Reif: Problem bei GISA
Wir prüfen nicht Seriennummer und Aussteller; dadurch gibt es keine Probleme beim Wechsel von Zertifikaten. Da sich der Issuer ändert, sind Änderungen notwendig.
BMI stellt kostenloses Beispielzertifikat zur Verfügung.

Wunsch:

- Zugriff auf bereits ausgestellte Zertifikate soll möglich sein. BMI wird Umsetzungswunsch prüfen.
- Liste welche Zertifikate als nächstes ablaufen. BMI wird Umsetzungswunsch nicht prüfen.

Stmk: Zertifikat läuft Anfang Februar aus; würden den öffentlichen Schlüssel des neuen Zertifikats zum Test zur Verfügung stellen.
BMI stellt öffentliche Teile div. Zertifikate zur Verfügung.

Neue BMI Zertifikate ist standardmäßig 2 Jahre gültig.

Zur Info: Gondor-Portal Läuft als Migrationsportal.
Jeder mit neuem Zertifikat wird aufs neue AWP Standardportal umgestellt. Partner müssen natürlich informiert werden. Kundmachung erfolgen in der PAI.

Daher: Bitte um rechtzeitige Information, wann ein Zertifikat ausläuft.
Hörbe: Wenn kein IBM Portal soll die ganze Zertifikatskette mitgesendet werden.

TOP 9: VKZ für die Bildungsdirektionen (Müller)

Information über das neue VKZ für die Bildungsdirektionen mit anschließender Diskussion der Participant-ID für Bildungsdirektionen:

Für die Bildungsdirektionen wurde eine neue Ebene M = Gemeinsame Behörde eingerichtet und der VKZ-Bereich für die Bildungsdirektionen wurde mit MBD festgelegt - siehe auch Email "WG: Verwaltungskennzeichen für Bildungsdirektionen".
Dies passt zu der Tatsache, dass diese neue Behörde Bundes- und Landesrecht vollzieht, stellt uns mM nach jedoch bzgl. der ParticipantID vor die Aufgabe, gleich zu Beginn die Frage, mit welcher Participant-ID die Mitarbeiter der Bildungsdirektion auftreten (und noch einige andere Dinge), zu klären, um etwaige zukünftige Probleme bzgl. unterschiedlicher Auffassungen zu verhindern.

Diskussionspunkte Portal / ParticipantID:
- Ausgangssituation: In der Bildungsdirektion arbeiten sowohl Bundes- als auch Landesbedienstete, welche jeweils Bundes- oder Landesrecht vollziehen können
- Muss die Bildungsdirektion (1x oder jede einzeln?) überhaupt dem Portalverbund beitreten?
- Unter welcher Participant-ID treten diese auf? Einer eigenen, der Participant-ID des jew. Landes, der Participant-ID des BMBWF?

In der Steiermark wäre der Einsatz des steiermärkischen Portals vorgesehen - mit Participant-ID AT:L6
Ziel der Diskussion ist es, hier gleich zu Beginn ein einheitliches Vorgehen zu finden.

Vorgehen / Beschluss

Jede Bildungsdirektion muss dem Portalverbund beitreten.

Frage zur Participant-ID wird am 12.12. in die AG-RESI übernommen.

Läuft auf einen eigenen Participant/zugriffsberechtigte Stelle für jede Bildungsdirektion hinaus. Zeitnahe Entscheidung notwendig, da die Umstellung im Jänner erfolgen muss. Beantragung eines Behördenkennzeichens ebenfalls notwendig.

Anmerkung AG-IZ: Die Participant-ID wurde mit email vom 19.12. versendet. Demzufolge würde die neue Participant-ID wie folgt lauten: AT:VKZ:MBD* (Rückmeldungen offen).

TOP 10: Portalverbund-CA der Stadt Wien (Müller)

Status Neue Portalverbund-CA der Stadt Wien:

Wie ist der Status dieser Umsetzung? Das TO war das letzte Mal im November 2017 auf der TO.
Weiters läuft die von BMI genutzte Zertifikatskette mit 1.12.2019 aus – schaffen wir den Wechsel vorher oder werden neue Wurzelzertifikate eingeführt? Die aktuell ausgestellten Zertifikate werden mit Gültigkeitsdauer 1 Jahr ausgestellt – kann man dies erhöhen?

Vorgehen / Beschluss

Die Neuausstellung von beantragten Zertifikat und Metadatenverwaltung sollen gemeinsam abgehandelt werden.

Authentisierung: MOA-ID mit Bürgerkarte oder ?

Pichler: Sobald SAML in Verwendung brauchen auch Anwendungen Portalverbundzertifikate (2 – eines zum Verschlüsseln, eines zum Signieren?)
Hörbe: kein Zwang zur Verwendung von 2 eigenen Zertifikaten; da beide private Schlüssel im Speicher – kein Sicherheitsgewinn.

TOP 11: PAI – Aktueller Fehlerstand (Stradal)

Klärung der letzten offenen Punkte (Siehe Mailverkehr der letzten Tage)

Letzter offener (kosmetischer) Fehler:
Bei der PDF-Generierung sind keine Rollen enthalten / unvollständige Informationen.
Ist kein einsatzverhindernder Fehler.

TOP 11: PAI – Formelle Abnahme (Stradal)

Finale formelle Abnahme

Ab sofort wird nur noch in der PAI publiziert.

Alte Anwendungen werden innerhalb der nächsten 6 Monate (bis 10.6.) in die PAI übernommen.

(z.B. Der Depositar (Scheidbach), informiert die Anwendungsverantwortlichen, sobald eine Anwendung, die neu publiziert werden soll, dass dies in der PAI erfolgen muss)

TOP 11: PAI – Trennung der Daten (Sachs-Gabitzer)

Aktuell ist die PAI nicht ideal für die Anwendungsverantwortlichen auszufüllen.
Wäre es möglich die organisatorischen Daten deutlich von den technischen Daten zu trennen?
Erfassungsmaske in 2 aufteilen oder wie sieht die Roadmap der Zentralen Dienste aus?

Sachs-Gabitzer nicht anwesend: wird in der nächsten AG-IZ besprochen.

TOP 11: Frist zur Meldung der Anwendungen in der PAI (Müller)

Aus der letzten AG-IZ, unter Berücksichtigung des aktuellen Standes

In der AG-IZ vom 1.2. haben wir beschlossen, dass bis 6 Monate nach Veröffentlichung des Protokolls die Anwendungen in der PAI zu erfassen sind. Das wäre demnach bis 12.8.2018. Die Frage die sich stellt, ist ob diese Frist im Rahmen der Sitzung/des Protokolls ausreichend ist, damit alle Anwendungsbetreiber darüber in Kenntnis gelangen. Besser wäre, wenn hier ein E-Mail von zentraler Stelle mit der Aufforderung zur Erfassung und der Frist versendet wird (lt. Hildegard Freidl war zu Beginn des Projekts vorgesehen, dass dies das BKA - nun wahrscheinlich BMDW - macht).

Ergebnis: wird aus letzten Sitzung übernommen.

TOP 11: PAI – Einbindung ReferenceServer (Müller)

Einbindung PAI Übersicht aller Anwendungen am alten ReferenceServer:

Der PAI-Aufruf der öffentlichen Liste der PV Anwendungen (https://portal.lfrz.at/at.gv.lfrz.pai-p/application_summary?doPdf=true) sollte auf dieser Seite mit einer kurzen Erklärung ergänzt werden: https://www.ref.gv.at/UEbersicht-aller-Anwendungen.1219.0.html, damit in der Übergangszeit auch wirklich alle Anwendungen am Referenzserver auffindbar sind. Zusätzlich sollte auch auf der Seite der „Betriebshandbücher für E-Government-Anwendungen“ ein kurzer Hinweis auf die PAI gestellt werden, da auch diese Liste nicht mehr vollständig ist.

Vorgehen / Beschluss

Bisherige Liste mit Betriebshandbüchern bis 10.6.2019 gültig. Danach wird das Dokument nicht mehr gewartet.

PAI gilt ab sofort und „überschreibt“ alles was im alten Dokument enthalten ist.
„PAI vor PDF“: zuerst in der PAI nachsehen, falls dort nichts vorhanden ist, im PDF nachsehen.
Klauser formuliert den Text dazu für den Reference-Server.

TOP 12: Publikation Dokument (Wittmann)

Status der publizierten Dokumente (LDAP, PVP)

Vorgehen / Beschluss

Dokumente wurden über die Verbindungsstelle ausgesendet. Müssen noch auf dem Reference-Server (ref.gv.at) eingetragen werden.

TOP 13: JAVA Umgebung (Reisinger)

Welche Portalverbundanwendungen benötigen am Client eine installierte Java-Runtime?

Hintergrund ist die leidige Lizenzdiskussion (aktuelles Java mit Support bei Oracle wird kostenpflichtig).

Wir wollen im Burgenland auf OpenJDK wechseln und würden gerne im Vorfeld so gut wie möglich die Kompatibilität testen. Nur ist es natürlich schwer, wenn man nicht weiss, welche der vielen Anwendungen Java am Client braucht.

Bekannt ist es mir z.B. bei der Anwendung für die Grundversorgung die auf SAP-Businessobjects basiert.

Vorgehen / Beschluss

Keine Hürden bekannt.

Anmerkung: Das Standardportal funktioniert unter OpenJDK.

TOP 14: Schema-Änderung gvApplIds (Minichshofer)

Aus unserer Sicht sollten die Sonderzeichen in gvApplIds auf ein notwendiges Minimum reduziert und auf den Stand vor der letzten Änderung des LDAP-Schemas zurückgestellt werden. Statt ":" und "/" sollte ein anderes (bisher auch gültiges) Zeichen (z.B. "_") verwendet werden. Auswirkungen auf die dahinter liegende Systeme (Reporting, Monitoring, etc.) sind für mich mit nicht abschätzbaren Aufwand verbunden.

Vorgehen / Beschluss
Div. Zeichen könnten bei Auswertungs- und Monitoring-Systemen Probleme machen. Einheitliches Schema wäre wünschenswert.

z.B. ZMR
oder at.gv.ooe.bmi präfix
oder @lfrz anhängen

Anwendungen in r- oder s-Profil müssen rein praktikabel entsprechend oft angelegt werden.

Diskussion des Attributs in der SubAG-PVP.
Ist nicht einsatzverhindernd für die PAI.

In der AG-IZ wurde folgendes beschlossen:

Für die gvApplIDs im pv-ldap (PAI) gilt folgende Konvention:

> <Domäne in umgekehrter Notation>.ApplikationsID[<Zusatz>]

Beispiele:

> at.gv.bmxy.app1-p
> at.gv.wien.gisa-wiki.awp

Das Feld gvUrlMapping im Objekt gvApplication ist für R-Profil-Anwendungen auf den Wert zu setzen, der in einem auf die Applikation verweisenden gvApplicationProxy-Objekt eines Stammportals zu verwenden ist.

TOP 15: Webtool Lehrpraxenförderung (Minichshofer)

Vom Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz hat eine Fachabteilung die Aufforderung bekommen sich auf einer Seite (https://fla.ehealth.gv.at) mittels Bürgerkarte anzumelden.
Aus unserer Sicht sollten solche Anwendungen über Portalverbund für Länder angeboten werden.

Vorgehen / Beschluss

Vorgehen soll in der AG-Leiter diskutiert werden.

TOP 16: Allfälliges

Allfällige Punkte der Teilnehmer:

Auswirkungen von PV-Spezifikationsänderungen auf PV Services (PAI, Zentrale Dienste): (Müller)

In Version 1.6.2 der LDAP_PV haben sich die erlaubten Zeichen für gvApplication/gvApplId geändert. Dadurch ist der Umstand entstanden, dass nun Anwendungen mit einer gvApplId (Version 1.6.2 – inkl. /) in dem LDAP enthalten sind, auf welches die PAI zugreift, die Logik der PAI diesen erweiterten Zeichensatz jedoch noch nicht unterstützt.
Künftig werden wir dieses Problem mM auch bei den zentralen Diensten (ZD) haben. Bitte daher um Diskussion, wie wir mit solchen Änderungen an den Spezifikationen umgehen. Folgende Stichworte/Fragen als erster Input zur Diskussion:

- Definierte LDAP Version, mit welcher die PAI/die ZD betrieben wird.
- Wie erfolgt die Replikation von abweichenden Versionen? Kann hier davon ausgegangen werden, dass das zentrale System (ZD oder PAI) die Version vorgibt und die jeweilige Gegenseite (zB die Länder) beim Abfragen aus dem zentralen System bzw. beim Befüllen desselbigen entsprechend konvertieren?
- Wie sieht es mit dem Wechsel auf eine höhere Version im zentralen System (ZD oder PAI) aus ◊ speziell die Auswirkungen auf Replikationen müssen durchdacht werden
- Aus Sicht der Datenqualität im zentralen System (ZD bzw. PAI) muss gewährleistet sein, dass die darin enthaltenen Daten alle derselben Version entsprechen und nicht je TN unterschiedlich sein können

>> siehe weiter oben.

Neue PVV mit Begriffsanpassungen an die DSGVO (Müller)
Die in der PVV geänderten Begrifflichkeiten (z.B. Auftragsverarbeiter statt Dienstleister) gemäß DSGVO müssen in einigen Dokumenten nachgezogen werden – z.B. Zugriff-DL, PVP Spec, ZD). Wer identifiziert diese Dokumente bzw. koordiniert die Anpassungen?

Ergebnis: Soll im Zuge der Aktualisierung des ref.gv.at passieren.
Vorab in der Übergangszeit kann eine Änderung des Glossars erfolgen.

Nächster Termin

Der nächste Termin: 7.3.2019, Ort wird bekannt gegeben.