Tagesordnung

Portokoll Sitzung AG-IZ

Datum: 28.05.2020, 10:00 – 16:00 Uhr
Ort: Videokonferenz

Teilnehmer:

Siehe AG-IZ-Teilnehmerliste 2020-05-28

Inhaltsübersicht

Inhalt

Top 1: Tagesordnung und Protokoll

Tagesordnung und letztes Protokoll

Vorgehen / Beschluss

Es gab keine Anmerkungen zum Protokoll der letzten Sitzung.

Top 2: Bericht Sub-AG Policy (Reif)

Bericht der letzten Sitzung Sub-AG Policy.

Vorgehen / Beschluss

Es hat keine Sitzungen stattgefunden.

Das Dokument PM-SMA 1.5 ist fertiggestellt. Im neuen Dokument gab es keine großen Änderungen, Das Dokument wird ab Juni wirksam.

Die Möglichkeit eines erneuten Scans der Portale zur Umsetzung der Vorgaben des Dokumente PV-SMA durch das EGIZ wurde diskutiert. Das LFRZ hat dazu ursprünglich ein Angebot gelegt, der aktuelle Scan sollte jedoch vom EGIZ durchgeführt werden. Das automatisierte Tool des EGIZ wurde nicht weiterverfolgt, kann wiederaufgenommen werden. Dominik Klauser nimmt das Thema mit.

Top 3: Bericht SubAG PVP (Lenz)

Bericht der letzten Sitzung der Sub-AG PVP.

Vorgehen / Beschluss

Peter Pichler berichtet in Vertretung von Thomas Lenz:

Thomas Lenz hat eine Version 2.2 von PVP erarbeitet. In dieser sind einerseits für die E-ID Lösung notwendigen Änderungen ins PVP Attribute Profil eingearbeitet worden. Zudem sind im Attribute Profil bereits Claim-Attribut-Namen für OIDC (Open-ID Connect) festgelegt worden.

Den Vorschlägen von Thomas Lenz wurde von der Sub-AG-PVP zugestimmt. Ein PVP-2-O-Profil (OIDC) gibt es noch nicht. Dieses soll geschafft werden, wenn die ersten Erfahrungen mit OIDC gesammelt wurden.

TOP 4: Bericht Sicherheitsklassen (Wittmann)

Statusbericht aktueller Stand des SecClass-Dokumentes:
Diskussion des vorab versendeten Dokumentes SecClass 4
Abnahme Dokument SC4 AG-IZ intern?

Vorgehen / Beschluss

Vom LFRZ kamen Anmerkung zu folgenden Punkten: Struktur und Umfang, Systemprincipal, eIDAS Inhalte

Komplexität: Es wurde innerhalb der Sub-AG beschlossen, die ursprüngliche Struktur der SecClass Version 3 (5 Dokumente) wieder auf ein Dokument zusammenzuführen.

Systemprincipal: Von STMK kamen Anmerkung: Falls es eine Möglichkeit gibt, den Chained Token auszuhebeln ist, besteht aus Sicht STMK Handlungsbedarf.

Im Entwurf wurde festgehalten: synchroner Aufruf → der Chained Token ist mitzuschicken, asynchron Aufruf → kein Chained Token, es gibt ein Problem bei der Protokollierung wenn das Ergebnis erst wesentlich später (z.B. ein paar Stunden) nach dem Aufruf verarbeitet wird.

Es wurden mehrere Möglichkeiten diskutiert:
.) Veranlassung der Änderung ist jedoch durch den User ausgegangen, wie loggt man das? → durch lokale Protokollierung (laut DSGVO).

.) Vorschlag STMK: AWP kann auswählen ob Chained Token notwendig ist oder nicht.

.) Vorschlag BMDW: Klarstellung durch genauere Definition des Datumsfelds (mit Zeit).

Anmerkung Wien: Erweiterung Chained Token um ursprünglichen Anforderungs-Zeitpunkt, Anmerkung OÖ: Unterscheidung ob Abfrage durch automatischen Job durchgeführt oder durch Person.

Anmerkung: asynchron und Batch sind unterschiedlich: asynchron wird vom User angestoßen und später durchgeführt, Batch automatisch durch ein System angestoßen

Lösungsvorschlag 1: Dreiteilung, syncrhon passt, asynchron durch Anwendung vorzugeben, Batch kein Chained Token.

Lösungsvorschlag 2: den dritten Punkt anpassen: Wenn Aufruf durch einen User, dann Chained Token (das Wort synchron aus dem Satz raus, bzw. synchron Und asynchron schreiben)

Rückfrage LFRZ: Definition Systemprincipal und dessen Sicherheitsklasse
Fazit: Systemprincipal hat keine Sicherheitsklasse. Prüfung der Sicherheitsklasse durch die Anwendung zu erfolgen.
Problem technisch: der Systemprincipal braucht dennoch eine Zahl. Entweder 3 oder 9, oder er erhält 2 oder 3 je nachdem wie der Webserver abgesichert ist.
Lösung: Sicherheitsklasse für Systemprincipal ist adäquat zu setzen

Anmerkung OÖ zu LoA: Aufteilung in Einzelübersichten (nach LoA)
BMDW: passt, wer es umsetzt wird noch geklärt.

Anmerkung STMK zu Seite 7: Statt Anwendung sperren nur Anwendungsrecht sperren, wird umgesetzt.

Weiteres Vorgehen: Änderungen werden eingearbeitet, Dokument nochmal ausgeschickt und über Umlaufbeschluss abgenommen.

TOP 5: Bericht Status Zentrale Dienste (Reif)

Statusbericht Peter Reif zur Produktivsetzung der zentralen Dienste

Vorgehen / Beschluss

Nächster Schritt: Übernahme des Testservers von Rainer Hörbe zur Stadt Wien (Plan Juni - Nachtrag zur Sitzung: ist mit 9. Juni 2020 erfolgt), dann Testphase und Produktivsetzung (Plan Oktober).

Nochmal kurze Zusammenfassung: Das Service (Metadatenverwaltung) dient der zentralen Verwaltung von SAML Metadaten und Client Zertifikaten der Stammportale. Teilnehmerverwaltung ist auch ein Teil.
Vorarlberg, OÖ, Tirol verwendet schon die Testinstanz (Hörbe). BKA plant es (zu berücksichtigen bei Umlage auf Wien)
Sobald es in der Testphase etwas zum Anschauen gibt, folgt eine Information

Blick in die Zukunft: Es stehen auch schon nächste Erweiterungen an, wie z.B. OpenID-Connect Metadaten

Parallel zu betrachten: Inhalt des formalen Auftrags AG-Leitung

Anmerkung OÖ: Bereits im Testsystem eingemeldeten Daten bitte prüfen, ob alles korrekt eingegeben wurde (Bspl. Discovery)

TOP 6: Aufbewahrungsfrist Revisionsprotokolle (Glock)

Es gibt keine ausdrückliche Festlegung in der PVV oder an anderer Stelle, wie lange Revisionsprotokolle aufbewahrt werden müssen. Die AG-IZ sollte sich auf eine verbindliche Frist einigen, zumindest im Sinne einer Best Practice.

Vorgehen / Beschluss

Anfrage aus NÖ: Wie lange müssen Revisionsprotokolle aufgehoben werden (nicht die Logs, sondern die Ergebnisse der jährlichen Sicherheitsrevision).
BMDW: Keine Festlegung niedergeschrieben, früher (Datenschutzgesetz) waren es 3 Jahre
Vorschlag: Aufhebungsdauer mind. 3 Jahre zurück; wird mit AG-RESI abgestimmt (WTA)

TOP 7: Abgleich ParticipantIDs mit ldap.gv.at (Glock)

Da ldap.gv.at als zentrales Verzeichnis von PV-Teilnehmern dienen soll, ist es unumgänglich, dass dort angegebene Daten - insbesondere die ParticipantId - aktuell gehalten werden und mit den Angaben übereinstimmen, die in lokalen Verzeichnissen geführt werden.

Vorgehen / Beschluss

Aufforderung des BMDW (Robert Glock): alle Portalbetreiber bitte ihre Daten in ldap.gv.at kontrollieren.

TOP 8: PAI - Status und Erweiterungen (Pesendorfer)

Als potentielle Erweiterungen sehe ich eine Verbesserung zur Anzeige der Anwendungs-Logos und die Erstellung von automatisierten Tests. Logos sind derzeit in der PAI nur für eigene Anwendungen sichtbar. Die Autotests fehlen beim Deployment neuer Versionen, zuletzt haben wir aufgrund von Problemen wieder auf die Vorversion wechseln müssen. Die Fehlersuche erfordert zusätzlichen Aufwand, der in der Betriebsgebühr nicht abgedeckt ist.

Erweiterungsideen für PAI:

- Anzeige des Logos in Anwendungsübersicht (Tabelle) und Betriebshandbuch
- Standardlogo für Mandanten (dieses soll angezeigt werden, wenn für eine gvApplication kein Logo vorhanden ist)
- Autotests für die wichtigsten PAI-Funktionen

Da Harald Stradal abwesend ist, sollte der Bedarf für diese Erweiterungen und die Finanzierungsmöglichkeit in der AG-IZ abgestimmt werden. Anschließend sollen die tatsächlichen Kosten erhoben und die Erweiterungen beauftrag werden.

Vorgehen / Beschluss

Aktuell V1.2.2 der PAI im Testsystem. Showstopper: LDIF Export nicht möglich. Rückmeldung an BMI durch Robert Glock.
Wer einen Zugriff aufs Testsystem möchte, bitte an LFRZ (Hans Jörg Möllner?) wenden.

Frage LFRZ: Sind alle mit den vorgeschlagenen Erweiterungen einverstanden, und wenn ja, wie sieht die Finanzierung aus?

Zusätzlicher Erweiterungswunsch: gvFederation Feld auch in PAI.

Vorschlag eines Termins: UseCases durchgehen und den verschiedenen Werkzeugen zuordnen (mind. Stadt Wien, LFRZ, BMI, wer noch möchte Mail an Robert Glock).

Anmerkungen Bild: in ldap.gv.at gibt es eine Spezifizierung von Logos, die sind in dem Zuge zu aktualisieren.

BMDW: Wenn alle Erweiterungen spezifiziert sind und ein Kostenvoranschlag des BMI vorliegt, kann es in der AG-Leiter diskutiert werden.

Anmerkungen zur PAI von BMDW:
Inaktive Anwendungen werden nicht automatisch gelöscht. Nach etwa 90 Tagen werden inaktive Anwendungen manuell aus der PAI gelöscht.

Bitte an BMDW: Kann eine Liste erstellt werden, wer wieviel Prozent eingemeldet hat?

TOP 9: Roadmap Zentrale Dienste (Glock)

Status Erstellung einer Roadmap „Zentrale Dienste“.

Vorgehen / Beschluss

Wurde in TOP5 behandelt

TOP 10: Allfälliges (Wittmann)

Allfällige Punkte der Teilnehmer

Vorgehen / Beschluss

TOP 10.1: Reference Server

Manche Teilnehmer haben das Problem, dass sich Dokumente nicht öffnen lassen (Bspl. Spezifikation LDAP unter Konventionen). Beim Aufruf der Public Seite funktionieren Dokumente. Wien bemüht sich um eine Behebung des Fehlers.

BMDW hat aktuell Schwierigkeiten alle Inhalte von Redaktion auf Live zu publizieren, soll im Juli übernommen werden.

Wenn generell noch Dokumente in der Konventionsliste (https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/konventionen-weitere-konzepte)fehlen, bitte Info an Hannes Wittmann, der die Infos gesammelt an Frau Maierhofer (BMDW) übermittelt.

Wer noch nicht in der ref.gv.at AG-IZ Gruppe ist, bitte Info an Hannes Wittmann, der die Einladung verschickt. Voraussetzung: Man muss sich zumindest einmal am Reference Server eingeloggt haben.

Nächster Termin

TOP für nächste AG-IZ: weiteres Vorgehen Liferay Gruppe AG-IZ und vieW4

Nächster Termin: 10.09.2020