

1. Frau St'in Haugg Lag vor, mit Dank zurück! Hö 2.12.

Über

Kopie: M, PSt JB, PSt MB, St P

Herrn AL L

Herrn AL 4

Frau UAL'in 43

Leiterin Task Force Entlastungspaket

mit der Bitte um Zustimmung und Verwendung

Betr.: Studierenden-Energiepreispauschalengesetz (EPPSG)

hier: Leitungsgespräch mit St Schlömer (Sachsen-Anhalt)

Bezug: Anforderung von St'in Haugg vom 29.11. sowie Herrn AL L vom 25.11.2022

Anlg.: 7

für IFG-Antrag relevante zwei Anlagen auf
den nachfolgenden Seiten
(Gesprächsvorbereitung und
"Entscheidungsbedarfe IT-Verfahren")

2. Vermerk

St Schlömer aus Sachsen-Anhalt (ST) hat um einen Gesprächstermin mit Frau Ministerin zur Umsetzung des EPPSG, insb. zur Antragsplattform, gebeten. Bund und Länder haben ein gemeinsames Zusammenwirken bei der Erstellung der Antragsplattform vereinbart und eine Bund-Länder-AG gegründet. Aufbau und Betrieb der Plattform sollen im Rahmen der bewährten Prozesse und Strukturen der OZG-Umsetzung im Themenfeld Bildung erfolgen. BMBF und ST sind hier gemeinsame Themenfeldführer und daher auch in der aktuellen Konzeptionsphase der Plattform gemeinsame Federführer.

Aus Anlass der genannten Gesprächsbitte findet am 30.11. von 16:00 bis 17:00 Uhr in Berlin ein Gespräch zwischen St Schlömer und Frau St'in Haugg statt. Folgende die aktuelle Konzeptionsphase der Antragsplattform betreffende Themen wurden benannt:

- Datenschutz,
- Zentraler Auszahlungsweg,
- IT-Verfahren und Sicherheitsniveau sowie
- Frage der Federführung in „Phase 2“.

In diesen Deckvermerk werden mit dem Ziel der Übersichtlichkeit lediglich die Gesprächsziele und Kernbotschaften zu den einzelnen Themen aufgenommen und für Gesprächsführung und Hintergrund auf jeweils beigefügte Gesprächsführungsvorschläge und Hintergrundinformationen verwiesen.

Datenschutz – Gesprächsziele / Votum

- Die konkreten Datenverarbeitungsvorgänge bei der IT-Plattform werden derzeit gemeinsam von ST, [init] und dem BMBF erarbeitet. Eine Verarbeitungsgrundlage im EPPSG, die den Anforderungen an die Normenklarheit genügt hätte, war in diesem Stadium nicht realisierbar. Es ist nicht möglich, eine Grundlage für im Detail noch unbekannte Datenverarbeitungsvorgänge zu schaffen.
- Es wird darauf ankommen, die bestehenden rechtlichen Verarbeitungsgrundlagen zu nutzen und die Konzeption der Plattform entsprechend datenschutzkonform auszugestalten.
- ST und BMBF haben vereinbart, dass zum Datenschutz Rechtsberatung eingeholt werden soll, BMBF dankt ST für Beauftragung der Kanzlei Redeker
 - Zu prüfen ist insbesondere, ob ein IT-Modell mit zentralem Datenabgleich auf der Plattform datenschutzrechtlich realisierbar wäre.
 - Weitere Optionen sollten geprüft und auch in der Bund-Länder-Runde am Donnerstag vorgestellt werden. [init] hat entsprechende Folien erarbeitet. Hier ist auch ein Modell vorgesehen, in dem die Prüfung der erstmalig durch die Antragstellenden eingegebenen Daten erst nachgelagert durch die Ausbildungsstätten geprüft wird. Die Arbeitsebene sollte dieses Modell verstärkt in den Blick nehmen.
- Ausführlicher Gesprächsführungsvorschlag in Anlage 1

Bundeskasse – Gesprächsziele / Votum

- BMBF wirbt bei Sachsen-Anhalt um wohlwollende und zeitnahe Prüfung, ob die Auszahlung der Einmalzahlung über eine Kasse des Landes Sachsen-Anhalt (z. B. Investitionsbank) erfolgen kann.
- Auszahlung über Bundeskasse wurde geprüft, hat sich als nicht realisierbar erwiesen. Sowohl eine Direktanbindung des Fachverfahrens an die Bundeskasse als auch eine Abwicklung analog zum Vorschuss bei der Überbrückungshilfe über die BAFA sind nicht umsetzbar.
- Gesprächsführungsvorschlag in Anlage 2a
- Gesprächsführungsvorschlag von Z21 zur Auszahlung über die Bundeskasse in Anlage 2b

Plattformmodell, IT-Verfahren und Sicherheitsniveau – Gesprächsziele / Voten

- Die verschiedenen Modelle der Plattform erfordern unterschiedliche Anforderungen an die Authentifizierung der Identität der Antragstellenden bei Antragstellung.
- Es wird darum gehen, die verschiedenen Verfahren auch in ihren Abhängigkeiten gegenüberzustellen, d.h. die Frage der Authentifizierung kann nicht pauschal beantwortet werden. Die Frage „wie“ authentifiziert wird, hängt u.a. vom gewählten Modell ab.
- Wir streben eine praktikable Lösung an. Es wird Aufgabe im weiteren Konzeptionierungsprozess der Plattform sein, hier das Spannungsverhältnis zwischen Nutzerfreundlichkeit und Risikominimierung aufzulösen.
- ~~Auch im Hinblick auf den Datenschutz sollte [init] in Bund Länder AG am 1.12. zusätzlich ein mögliches Alternativmodell in zwei Varianten vorstellen:~~
- ~~Modell 1: Vorab-Zusammenführung und zentraler Datenabgleich auf der Plattform~~

○ Modell 2: wie Modell 1, aber mit verschlüsselten Daten

- Modell 3: Prüfung der erstmalig durch die Antragstellenden eingegebenen Daten erst nachgelagert durch die Ausbildungsstätten, ggf. Absicherung durch verschlüsselten Token. Um den avisierten Starttermins der Plattform nicht zu gefährden, hat sich ST nach vertiefter Prüfung am 29.11 für ein Verfahren unter Nutzung der (bBund.idID+Token)-ausgesprochen (Identifizierung mit Online-Ausweis oder ELSTER-Zertifikat). Hierbei wird insbesondere die hohe Nachnutzbarkeit der BMWK Plattform berücksichtigt. [Verwendung BundID voraus. auch datenschutzrechtlich vorteilhaft, da Rechtsgrundlagen für Datenverarbeitung im OZG anwendbar.]
- Nach erster (fachlicher) Einschätzung ist die Verwendung der BundID zur Authentifizierung der Identität der Antragstellenden. Dieses Zielbild ist für uns fachlich nachvollziehbar und zustimmungsfähig.

- Ausführlicher Gesprächsführungsvorschlag in Anlage 3a
- Von jinit[erstellte Präsentation der Prozessvarianten in Anlage 3b
- Übersicht über Entscheidungsbedarfe zum IT Verfahren in Anlage 3c

„Phase 2“ – Gesprächsziele / Voten

- Bekräftigung, dass Bund zu seinen Zusagen steht und Pilotbetrieb (bis Ende 2023) finanziert (unter den oben skizzierten Maßgaben).
 - Engagement von Sachsen-Anhalt im Rahmen der Projektarbeiten und gute Zusammenarbeit würdigen.
 - Dank an Sachsen-Anhalt, dass Entwicklung der Plattform (Phase 1) durch das Land zügig beauftragt wurde.
 - Frühzeitiges Einvernehmen auf Leitungsebene herstellen, dass ST/MID auch Beauftragung und Umsetzung des Pilotbetriebs übernimmt (Zusage von Arbeitsebene liegt vor).
 - Sensibilisierung für Kostenrahmen (Eilbedürftigkeit darf nicht zu überhöhten Kosten für Betrieb führen, kleiner Aufschlag ist aufgrund der Umstände ggf. hinzunehmen und gegen Aufwand bei Wechsel des IT-Dienstleisters abzuwägen).
- Ausführlicher Gesprächsführungsvorschlag in Anlage 4

3. Wv.: Taskforce

Z 13	Z 21	122	UAL 41	ISM
<u>NR 29.11.22</u>	<u>Lee, 29.11</u>	<u>K.g. 29/11</u>	<u>Greisler, 29.11.22</u>	<u>PRo, 29/11</u>

4. Kopien: L 13

gez. Maxin

Z21: Auszahlung via Bundeskasse erscheint unrealistisch, s. im Einzelnen Anlagen 2.

BMBF	Terminvorbereitung	Datum: 30.11.22
Referat:	Anlass: Gespräch StH mit St Schlömer (ST)	
Taskforce	am: 30.11.2022	
Bearbeiter/in:	in:	
Taskforce / Renz	Tagesordnungspunkt Nr.:	
Hausruf:	betrifft: IT-Verfahren und Informationssicherheit	
Aktenzeichen:	Unterlagen: Foliensatz Init	

Gesprächsziel

- Entscheidung der offenen Fragen zur Auswahl eines bevorzugten IT-Verfahrens anhand des Vorschlags ST
- Votum: Zustimmung zum vorgeschlagenen Verfahren
- Dieses ist notwendig, um die Umsetzung der entsprechenden Komponenten des Verfahrens beginnen zu können-
- Zustimmung zur weiteren engen fachlichen Begleitung der genauen operativen Ausgestaltung des Verfahrens, unter anderen durch Beteiligung des BMBF (Herr Renz) in der hierzu eingesetzten Arbeitsgruppe
- Wunsch das Verfahren bei Bedarf anhand des Feedbacks später zu erweitern

Vorschlag zur Gesprächsführung

- Erläuterung der Vor- und Nachteile und Herstellen eines gemeinschaftlich von Bund und Ländern sowie den Stakeholdern akzeptierten Verfahrens mit Fokus auf den vorliegenden Verfahrensvorschlag.
- Risiken (IT Sicherheit, Projektstart) und die Nutzendenfreundlichkeit sind miteinander in Einklang zu bringen

Sachstand / Hintergrund

- Nach weiterer vertiefter Prüfung durch ST kam am 29.11 der Verfahrensvorschlag mit Nutzung von Bund ID (eID/Elster) zur Anmeldung und Token zur Prüfung der Berechtigung
- Ein zentrales Argument für diese Auswahl (die von der ursprünglich von ST favorisierten Auswahl abweicht) ist die Nachnutzung der vorhandenen Plattform und damit die Risikominimierung einer verspäteten Bereitstellung, also das Erreichen des Launch Zeitpunktes
- Es wurde sich hier damit gleichzeitig für die maximale Sicherheit der Authentifizierung entschieden
- Das Onboarding der Antragstellenden in bund.id/Servicekonten ist aufwendiger als die Nutzung vorhandener Wege wie DFN-AAI, dies ist aber nur einmalig zu machen und kann nachfolgend auch für weitere Verwaltungsdienstleistungen genutzt werden
- Die spätere Erweiterung des Verfahren halten wir uns grundsätzlich offen.
- BMBF nimmt an Technik AG teil um Prozess eng zu begleiten

Wie in M-Vorlage vom 21.11 (Elva 2022-47820) ursprünglich geschildert und inzwischen im Foliensatz von init weiter spezifiziert gibt es grundsätzlich drei verschiedene Verfahrensansätze.

Modell 1 (Token unverschlüsselt):

Im ersten Model (Variante 1) erfolgt eine lokale Tokengenerierung in den Ausbildungsstätten (per Excel oder einem niedrigschwelligen Hilfsmittel), diese werden dann durch die Landesbeauftragten der Plattform mandantenspezifisch zur Verfügung gestellt. Dieses Verfahren wird im Foliensatz ab Seite 8 als genauer erläutert.

Modell 2 (Token verschlüsselt):

Das Model 2 ist vom Ablauf her identisch, die Daten werden dabei aber verschlüsselt übertragen. Der Token dient hierbei als Schlüssel. Nur wer in seinem Besitz ist (also lediglich die Ausbildungsstätte und der Antragstellende) kann somit auf die Daten zugreifen (Foliensatz Folie 16ff). Bei Eingabe/Übergabe des Tokens durch den Antragsteller werden die Daten auf dem Server automatisch entschlüsselt.

Ein Einsehen der personenbezogenen Daten vor Antragstellung durch Plattformbetreiber oder den Bund ist nicht möglich.

Modell 3 (Listenprüfung):

Modell 3 (von Task Force aus Datenschutzgründen favorisiert): In diesem Modell erfolgt die Prüfung der erstmalig durch die Antragstellenden eingegebenen Daten erst nachgelagert durch die Ausbildungsstätten. Damit diese Prüfung auf Basis verlässlicher Information erfolgen kann, ist in diesem Szenario zwingend die Verknüpfung mit nachprüfbaren Informationen über die Identität des Antragstellenden herzustellen. Nachteile sind hier eine längere Bearbeitungszeit

Während bei Hochschulen für die Authentifizierung etablierte Verfahren (Shibboleth/DFN-AAI) existieren, ist das Bild bei Fachoberschulen heterogener, hier kann nicht auf übergreifende Lösungen zurückgegriffen werden, so dass hier der Einsatz von bund.id (also Anmeldung via Personalausweis oder Elsterzertifikat) oder Verfahren wie Tan Briefe notwendig sind. In diesem Szenario müsste man sich dann für ein Verfahren entscheiden, welches priorisiert umgesetzt werden soll. Dieses Verfahren wird im Foliensatz ab Seite 16 genauer erläutert.

Alle genannten Verfahren sind immer in Kombination mit der Authentifizierung zu betrachten:

 Bundesministerium für Bildung und Forschung		Authentifizierung	
		bund.id (eId, Elster)	2FA (Email, DFN-AAI, SMS, Shared Knowledge)
		Nur dieses Verfahren garantiert ein sicheres Identifizieren der Antragstellenden inkl. Stammdaten (Vorname, Name, Geburtsdatum), benötigt aber Perso+Pin bzw. Elsterzertifikat hat damit hohe Hürden für die Nutzenden. Doppelbeantragung nicht möglich.	Um die Identität des Antragstellenden nachzuvollziehen kann auf bekannten Kommunikationskanal oder Merkmale zurückgegriffen werden. Dies ist weniger sicher, aber dafür einfacher . Dieses Merkmal ist als Teil der Listen vorab zu übermitteln oder müssen im Nachhinein durch die Ausbildungsstätten prüfbar sein und somit dort vorliegen.
		Mögliche Variante , aber noch keine Klärung der Passfähigkeit der Aufgaben der beteiligten Stakeholder. Langsamer für Nutzende.	Keine Sicherung des Verfahrens, dadurch enormer Prüfaufwand auf Basis nicht sicher erhobener Daten. → Nicht empfohlene Kombination
Autorisierung	Listenprüfung	Ausbildungsstätte prüft regelmäßig (via Landeskoordinator) zugestellte Liste gegen dort intern vorliegende Liste/Datenbank der Berechtigten, Datenverarbeitung auf Basis Einwilligung	
	Token	Personalisierte Berechtigungstoken werden vorab durch Ausbildungsstätte erstellt und werden mit personenbezogenen Daten (ggf. verschlüsselt) je Land im Portal hinterlegt, zusätzlich datenschutzrechtliche Klärung erforderlich	Mögliche Variante , aber noch Klärung Datenschutz-Grundlage und Anforderungen (Verschlüsselung) durch Länder notwendig. Mögliche Variante . Alternative oder ergänzende Ausprägungen (je nach Datenlage/Konzept). Verdachtserkennung von Doppelbeantragungen über IBAN und/oder personenbezog. Merkmale möglich. Absicherung durch vorab übermittelten Kommunikationskanal (Email, SMS) oder SSO. und / oder Absicherung durch dem Antragstellenden bekannte Merkmale (bspw. Matrikelnr. + Geburtsdatum).

Bewertung der Varianten

Wir streben eine praktikable Lösung an. Es wird Aufgabe im weiteren Konzeptionierungsprozess der Plattform sein, hier das Spannungsverhältnis zwischen Nutzerfreundlichkeit und Risikominimierung aufzulösen.

Pst J. Brandenburg schreibt zu den Modellen hierzu im Rücklauf unter Zustimmung von M in oben genannter M-Vorlage: „im Vordergrund steht die schnellstmögliche Umsetzbarkeit. Wenn die Authentifizierung der Antragstellenden (zusätzlich zur Kenntnis der Matrikelnummer etc.) bereits durch einen Token gewährleistet ist, sollte auf ein zusätzliches Elster-Zertifikat im Sinne einer niedrigschwelligen Antragstellung verzichtet werden.“

Unter dieser Zielprämisse wäre Variante 2 nur mithilfe von vorher übermitteln personenbezogener Informationen für Fachschulen sicher umsetzbar, womit sich die gleichen datenschutzseitigen Herausforderungen wie bei Variante 1 stellen, der wesentliche Vorteil der Variante entfällt somit.

Da Authentifizierung (Wer bin ich) und Autorisierung (Bin ich berechtigt die Prämie zu bekommen) nicht getrennt betrachtet werden können, bleiben somit **drei mögliche Kombinationen**:

Varianten	Verfahren	Vorteile	Nachteile
Model 1/2 (im Schaubild unten rechts)	Token mit 2. Faktor	Pragmatische Version mit vermutlich hinreichender Sicherheit, Verschlüsselung ratsam (Modell 2)	Datenschutzeinschätzung durch ST bzw. Rechtsgrundlage (Verordnung) ausstehend
Modell 3 (im Schaubild oben links)	Listenprüfung mit bund.id (plus Servicekonten) bzw. optional Shibboleth	Wenig Datenschutz	Hohe Barriere für Nutzenden, keine direkte Prüfung

Model 2 mit bund.id (im Schaubild unten links)	Token mit bund.id	Maximale Sicherheit, Hohe Wiederverwendbarkeit der Plattform	Hohe Barriere für Nutzenden
--	-------------------	---	--------------------------------

Votum:

Das Model 2 (Token) in Verbindung mit einer Tokenlösung ist das von ST nach vertiefter Prüfung bevorzugte Modell. Insbesondere unter Berücksichtigung der Wichtigkeit einen zeitnahen Beginn des Antragverfahrens ist diese Auswahl sinnvoll, da hier der Nachnutzungsfaktor der bestehenden Plattform und Komponenten am höchsten ist.

Die Umsetzung mit neuen Verfahren wie Shibboleth bringt Vorteile in Punkto Benutzerfreundlichkeit, ist aber nach nicht ohne erhebliche Risiken zum Start des Verfahrens umsetzbar.

Wir wollen uns solche Erweiterungen offenhalten und init wird hierfür ein Projektplan vorlegen.

Modell 3 ist bei nichterfüllen dieser Kriterien als Fallback das bevorzugte Szenario, erfordert ebenso ein sicheres Anmeldeverfahren wie bund.id. •

Die genaue operative Ausarbeitung des gewählten Modells sollte gemeinsam zwischen ST und Bund sowie dem Dienstleister unter Nutzung der existierenden engen Umsetzungsbegleitung (bspw. Daily) und unter Einbeziehung der großen Bund-Länder Runde erfolgen.

Reaktiv:

- Eine unverschlüsselte Übertragung (Model 1) sehen wir grundsätzlich kritisch, hier müssten zusätzliche Sicherheitsmechanismen diskutiert und etabliert werden.
- Sollten andere Verfahren oder Alternativen der Ausgestaltung im Gespräch aufgeführt werden, so stehen wir diesen grundsätzlich offen gegenüber, solange die Projektziele (Zeit, Einfachheit, Datenschutz und Sicherheit) nicht gefährdet werden, müssen diese aber einzeln prüfen.

Informationssicherheit:

Eine abschließende Bewertung durch das Informationssicherheitsmanagement des BMBF kann noch nicht getroffen werden, da hierfür neben der allgemeinen Prozess- und Architekturbeschreibung auch ein konkretes Implementierungskonzept vorliegen müsste, aus dem die einzelnen technischen und organisatorischen Sicherheitsmaßnahmen hervorgehen.

Berücksichtigung sollte bei der Modellauswahl unbedingt die **Technische Richtlinie des BSI zu elektronischen Identitäten und Vertrauensdiensten im E-Government (BSI TR-03107-1)** finden. Zwar ist eine TR nicht verbindlich, jedoch bildet sie die Best Practices und den Stand der Technik ab, der bei Authentisierung und Autorisierung eingehalten werden soll. Käme es zu einem Sicherheitsvorfall und wurde die TR-03107-1 nicht beachtet, könnte dies zu politischen Implikationen und einer negativen Außenwirkung führen. Im Kern verfolgt die TR einen risikobasierten Ansatz. Welche Authentisierungs- und Autorisierungsmittel zu verwenden sind – ob organisatorischer oder technischer Natur – und welche zusätzlichen Schutzvorkehrungen vorzunehmen sind, richtet sich nach dem Schutzbedarf des Verfahrens und den möglichen Gefährdungen. Insofern muss seitens der Taskforce bzw. dem Eigentümer des Verfahrens zunächst der Schutzbedarf bestimmt werden. Daraus ergibt sich dann die Kritikalität und diese bestimmt unter Informationssicherheitsgesichtspunkten die Wahl des Modells.

Grundsätzlich sind die Maßnahmen die sich positiv auf die Informationssicherheit auswirken (z. B. Verschlüsselung) auch vorteilhaft für den Datenschutz, da dieser eine Teilmenge der Informationssicherheit bildet.

Zu klären ist demnach zunächst und insbesondere, wer abschließend verantwortlich für die Informationssicherheit ist, also ob das BMBF hier im Sinne einer geteilten Verantwortung mitverantwortlich ist und demnach u. a. den o. g. Schutzbedarf zu bestimmen hat. Erst danach kann eine tragfähige Informationssicherheitskonzeption erstellt werden.

Zum Thema **IT-Sicherheit der Anbindung Kassenverfahren** ist derzeit ebenso wenig eine abschließende Bewertung durch das Informationssicherheitsmanagement des BMBF möglich. Die Skizze lässt nämlich aktuell kaum einen Rückschluss auf Sicherheitsmaßnahmen zu, so dass das Sicherheitsniveau nicht bewertet werden kann. Positiv ist die manuelle Prüfung der Liste der Rückmeldungen hervorzuheben, mit der organisatorisch ein Abgleich der zum Zahlungsexport bereitgestellten mit den tatsächlich zur Zahlung angewiesenen Vorgängen sichergestellt wird. Angaben dazu, ob bspw. die Mindeststandards des BSI in der Bundesverwaltung berücksichtigt wurden, falls ja, wie diese konkret umgesetzt wurden, welcher Schutzbedarf für die Dimensionen Vertraulichkeit, Integrität und Verfügbarkeit angelegt wurde, ob der IT-Grundschutz beim Design berücksichtigt wurde, etc. lassen sich dem Schaubild leider nicht entnehmen.



Bundesministerium
für Bildung
und Forschung

Entscheidungsbedarfe IT-Verfahren

bmbf.de





Bundesministerium
für Bildung
und Forschung

Authentifizierung

bund.id

(eId, Elster)

Nur dieses Verfahren garantiert ein **sicheres Identifizieren der Antragstellenden inkl. Stammdaten** (Vorname, Name, Geburtsdatum), benötigt aber Perso+Pin bzw. Elsterzertifikat hat damit hohe Hürden für die Nutzenden. Doppelbeantragung nicht möglich.

2FA

(Email, DFN-AAI, SMS, Shared Knowledge)

Um die Identität des Antragstellenden nachzuvollziehen kann auf bekannten Kommunikationskanal oder Merkmale zurückgegriffen werden. Dies ist **weniger sicher, aber dafür einfacher**. Dieses Merkmal ist als Teil der Listen vorab zu übermitteln oder müssen im Nachhinein durch die Ausbildungsstätten prüfbar sein und somit dort vorliegen.

Mögliche Variante, aber noch keine Klärung der Passfähigkeit der Aufgaben der beteiligten Stakeholder. Langsamer für Nutzende.

Keine Sicherung des Verfahrens, dadurch enormer Prüfaufwand auf Basis nicht sicher erhobener Daten.

→ **Nicht empfohlene Kombination**

Mögliche Variante, aber noch Klärung Datenschutz-Grundlage und Anforderungen (Verschlüsselung) durch Länder notwendig.

Mögliche Variante. Alternative oder ergänzende Ausprägungen (je nach Datenlage/Konzept). Verdachtserkennung von Doppelbeantragungen über IBAN und/oder personenbezog. Merkmale möglich.

Absicherung durch vorab übermittelten Kommunikationskanal (Email, SMS) oder SSO.

und / oder

Absicherung durch dem Antragstellenden bekannte Merkmale (bspw. Matrikelnr. + Geburtsdatum).

Autorisierung

Listenprüfung

Ausbildungsstätte prüft **regelmäßig** (via Landeskoordinator) **zugestellte Liste** gegen dort intern vorliegende Liste/Datenbank der Berechtigten, Datenverarbeitung auf Basis Einwilligung

Token

Personalisierte Berechtigungstoken werden **vorab durch Ausbildungsstätte erstellt** und werden mit personenbezogenen Daten (ggf. verschlüsselt) je Land im Portal hinterlegt, zusätzlich datenschutzrechtliche Klärung erforderlich

Von: Gerlach, Sonja /43
Gesendet: Freitag, 2. Dezember 2022 18:28
An: [REDACTED] (init); [REDACTED] (init)
Cc: Hasler, Jörn /L; Jörn Hasler; Schüller, Ulrich /4; Maxin, Falko /411; Höhne, Christiane /PeStH; [REDACTED]
Betreff: Rückmeldung bundID

Liebe [REDACTED],
lieber [REDACTED],

nach Freigabe durch die Hausleitung darf ich Ihnen folgende Rückmeldung übermitteln:

„BMBF stimmt Verwendung des Nutzerkontos Bund (BundID, bzw. interoperable Servicekonten der Länder) als ergänzender bzw. alternativer Authentifizierungsweg zu.

Wegen der teilweise hohen Hürden für die Nutzung der BundID sollen aus Sicht des BMBF nach Möglichkeit prioritär alternative, aus Sicht der Nutzenden vorteilhafte Authentifizierungswege zum Einsatz kommen. Hierzu zählt (vorbehaltlich der noch laufenden fachlichen und technischen Prüfung) insb. Shibboleth / DFN für voraussichtlich die große Mehrheit der Antragsberechtigten aus den Hochschulen. Daneben können durch die Ausbildungsstätte verifizierte Kommunikationswege (Email, SMS, Post), über die ein zweiter Token verschickt werden kann, zum Einsatz kommen. Ziel ist es, dass eine möglichst kleine Gruppe auf die Nutzung der BundID als alleinigen Authentifizierungsweg angewiesen ist. Zugleich ist mit Blick auf die unterschiedlich schnelle Umsetzbarkeit der verschiedenen Authentifizierungswege der Maßgabe eines möglichst frühen Starttermins für die Plattform Rechnung zu tragen.

Begleitend sollte frühzeitig mit vorbereitenden Kommunikationsmaßnahmen begonnen werden, um die Antragstellenden möglichst früh auf evt. Vorbereitungsmaßnahmen hinzuweisen und diese zeitlich vorziehen zu können (Einrichtung BundID, ELSTER-Zertifikat).

Insbesondere für kleinere Fachschulen und Berufsfachschulen sollen weitere pragmatische Szenarien geprüft werden, welche es ermöglichen auf den zweiten Faktor zu verzichten bzw. diesen durch eine Vor-Ort-Validierung oder Übergabe des Tokens zu ersetzen (Stichwort „Premiumtoken“). Präventiv ist zu prüfen, inwiefern der zweite Token auch verschickt werden kann, sollte aus Datenschutzgründen die Email-Adresse nicht bekannt sein, die Zugehörigkeit einer Email-Adresse aber über die Domain sichergestellt werden können.“

Viele Grüße
Sonja Gerlach

Dr. Sonja Gerlach

Unterabteilungsleiterin

Unterabteilung 43 - Bildungsfinanzierung

Bundesministerium für Bildung und Forschung

Heinemannstraße 2, 53175 Bonn | Postanschrift: 53170 Bonn

Tel.: +49 228 99 57-2367 | Fax: +49 228 99 57-82367 | Sonja.Gerlach@bmbf.bund.de

www.bmbf.de | www.twitter.com/bmbf_bund | www.facebook.com/bmbf.de |

www.instagram.com/bmbf.bund

Der Schutz Ihrer Daten ist uns wichtig. Nähere Informationen zum Umgang mit personenbezogenen Daten im BMBF können Sie der Datenschutzerklärung auf www.bmbf.de entnehmen.

Wenn ein Jinit[-Logo über
dem Bild liegen soll, dieses
im Jinit-Fahrer
entweder in der Karte
einfügen.

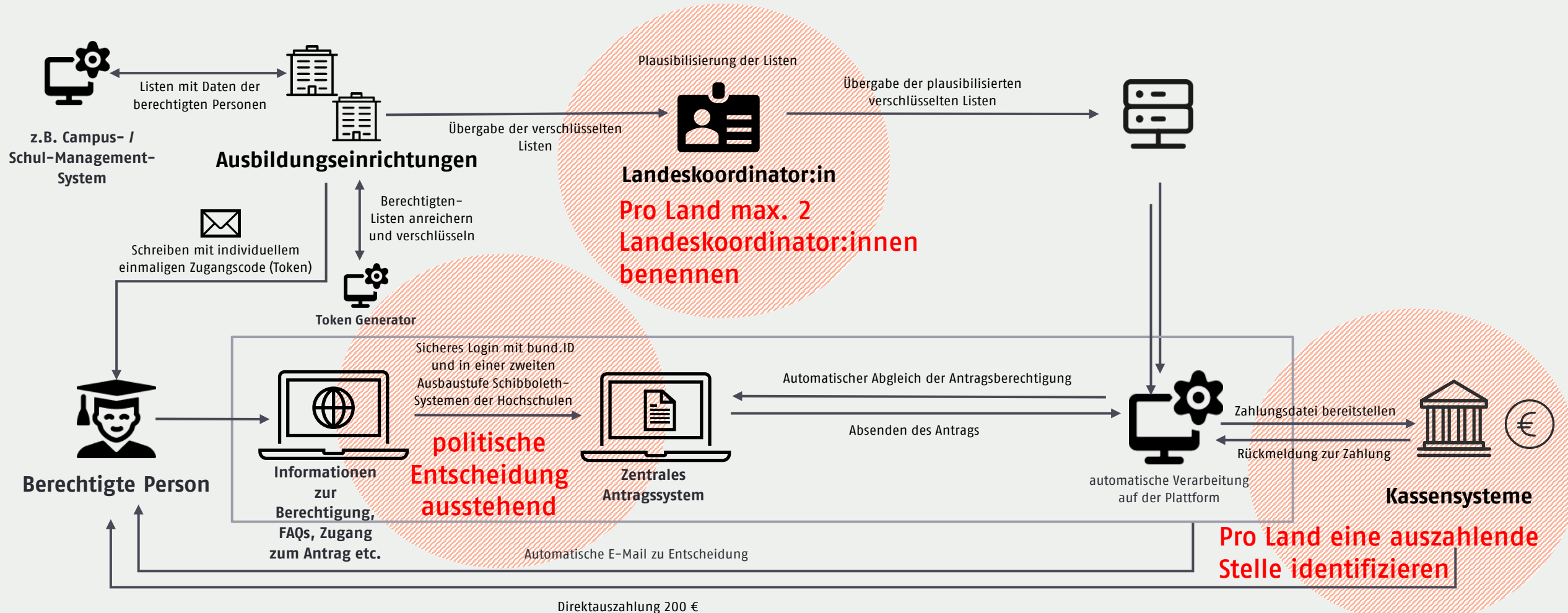
Jinit[-

Einmalzahlung nach EPPSG

Stand 01.12.2022

Schematischer Prozess – aktueller Stand

Antragsbasierter Ende-zu-Ende Ansatz



BMBF	Terminvorbereitung	Datum: 19.12.2022
Referat:	Anlass: BE-Gespräch	
Taskforce	am: 19.12.22	
Bearbeiter/in:	in: digital	
Busch	Tagesordnungspunkt Nr.:	
Hausruf: 3292	betrifft: Energiepreispauschale für Studierende, Fachschülerinnen und Fachschüler	
Aktenzeichen:	Unterlagen:	

Gesprächsziel

- Berichterstatte(r)innen und -erstatte(r) über den neuesten Stand des Projekts informieren.
- Vorstellung der unterschiedlichen Arbeitspakete, die derzeit bearbeitet werden.

Vorschlag zur Gesprächsführung

- Erfreulich: Das Gesetz wurde am Freitag (16.12.22) im Bundesrat ohne Einrufen des Vermittlungsausschusses gebilligt.
- Antrag des Landes Schleswig-Holstein auf Erweiterung des Berechtigtenkreises – Aufnahme von Grenzpendlern - im EPPSG hat im Bundesrat keine Mehrheit gefunden.
- *Reaktiv:* Schleswig-Holstein setzt eigenes Landesprogramm zur Entlastung von Grenzpendlern ein: [Hochschulen - Kiel - Studierende Grenzpendler bekommen Energiepauschale vom Land - Bildung - SZ.de \(sueddeutsche.de\)](https://www.sueddeutsche.de/hochschulen-kiel-studierende-grenzpendler-bekommen-energiepauschale-vom-land-bildung-sz.de)
- Ausgestaltung der Antragsplattform geht voran: Genaue Modalitäten der Authentifizierung noch nicht abschließend geklärt.
- Derzeit auf jeden Fall zwei Formen der Authentifizierung: BundID und Variante Code+Pin (insbesondere für kleinere (Berufs-)Fachschulen).
- Authentifizierung via Shibboleth hat sich aufgrund fehlender Umsetzungsmöglichkeit im Hochschulbereich zerschlagen (umfassendes Programm-Update erforderlich, nicht realistisch).
- Möglichkeit der Antragstellung durch Dritte kommt eher nicht – ST ist skeptisch.
- Zentrale Auszahlung noch in Prüfung. Derzeit favorisiert: Zentrale Auszahlung durch Investitionsbank Sachsen-Anhalt.
- Projekt-Governance ist eingesetzt. BMBF entzieht sich nicht der Verantwortung, sondern bringt zahlreiche Impulse in das Projekt ein.
- Vor Start der Einmalzahlung soll auf einer Info-Website schon einmal über die Modalitäten der Beantragung der Einmalzahlung informiert werden.
- Berechtigte können sich damit bereits vor Antragstellung über die Erfordernisse bei der Authentifizierung informieren und entsprechende Zugänge beantragen.

Sachstand / Hintergrund

1. Gesetzgebungsverfahren

Das Gesetz hat am 16.12.2022 den Bundesrat passiert und kann damit – wie vorgesehen – zum 21.12.2022 in Kraft treten.

Der Bund hatte den Ländern folgende Protokollerklärung angeboten:

„Die Bundesregierung sagt zu, die Länder beim Vollzug des Gesetzes mit einer digitalen Antragsplattform zu unterstützen. Die geplante digitale Antragsplattform nebst zugehöriger IT-gestützter Prozessketten wird den Ländern im Rahmen eines OZG-Umsetzungsprojekts zur Verfügung gestellt. Die Kosten der Plattform trägt der Bund.

Sollte im Rahmen der weiteren Entwicklung oder Inbetriebnahme der Antragsplattform zwingender datenschutzrechtlicher oder anderer Regelungsbedarf festgestellt werden, dem nicht auf Grundlage des EPPSG in der vorliegenden Fassung abgeholfen werden kann, wird die Bundesregierung eine einheitliche datenschutzrechtliche Regelung sowie mögliche weitere Regelungen im Rahmen der verfassungsrechtlichen Kompetenzen des Bundes für ein Änderungsgesetz vorlegen. Darüber hinaus wird der Bund für die Nutzung der Antragsplattform eine zentrale Auszahlungsstelle anbieten.“

Die Länder haben sich mit dieser PE einverstanden erklärt.

2. Antragsplattform

Die Arbeiten an der Antragsplattform gehen voran. Es wurde auf Leitungsebene ein Steuerungskreis für die strategischen Entscheidungen eingerichtet („Montagsrunde“), in dem Sachsen-Anhalt den Vorsitz hat. BMBF ist durch AL L plus eine weitere Person ebenfalls vertreten. Auf Arbeitsebene wurden Arbeitsgruppen gebildet, die die einzelnen Themen zur Umsetzung der Antragsplattform bearbeiten. Noch nicht eingesetzt, aber ebenfalls geplant, ist ein weiterer Kreis zur OZG-konformen Steuerung des Projekts. In diesem Kreis wird BMBF den Vorsitz haben.

3. Authentifizierung

Die anfangs in Betracht gezogene Haupt-Authentifizierung im Hochschulbereich via Shibboleth hat sich nachträglich als nicht-realisiert herausgestellt, da in fast allen Hochschulen hierzu ein System-Update erforderlich wäre. Damit wird eine Authentifizierung via BundID in den meisten Fällen voraussichtlich die Wahl sein, für kleinere (Berufs-)Fachschulen soll eine zweite Authentifizierung via Code + PIN vorgehalten werden. Der Code wird dabei – wie der Token/die Antragsberechtigtennummer – von der Schule ausgegeben, die PIN wird unter Auflagen (z. B. nur persönlich gegen Unterschrift) durch die Ausbildungsstätte an die anspruchsberechtigte Person übergeben, die Ausbildungsstätte muss sich zur Einhaltung dieser strikten Auflagen verpflichten. Mit dieser „niedrigschwelligen“ Authentifizierung sollen all diejenigen Fälle erfasst werden, bei denen eine Authentifizierung via BundID nicht in Betracht kommt.

4. Auszahlung

Eine zentrale Auszahlung der Einmalzahlung über die Investitionsbank Sachsen-Anhalt ist derzeit noch immer in Prüfung. Der Bund hat den Ländern in der Protokollerklärung eine zentrale Auszahlung angeboten. Sollte sich die Auszahlung über Sachsen-Anhalt zerschlagen, wird BMBF mit Sachsen-Anhalt die zentrale Auszahlung aus der Bundeskasse angehen. Hierfür gibt es drei Lösungswege:

- Direktanschluss der EPPSG-Plattform an die Bundeskasse nach entsprechender Ausnahmegenehmigung durch BMF und BRH, wobei Sachsen-Anhalt die Anträge für die Ausnahmegenehmigungen stellt.
- Direktanschluss der EPPSG-Plattform an die Bundeskasse nach entsprechender Ausnahmegenehmigung durch BMF und BRH, wobei BMBF die Anträge für die Ausnahmegenehmigungen stellt.
- Zwischenschaltung einer Bundesbehörde, analog zu den BMWK-Überbrückungshilfen, so dass die Zahldateien von einer bereits bei der Bundeskasse „zertifizierten“ Stelle weitergeleitet werden. Problem dürfte hierbei allerdings sein, dass BMBF keinen entsprechenden nachgeordneten Bereich hat, der ein solches Massenverfahren stemmen könnte (das BAFA hat aufgrund anderweitiger Aufgabenübertragung bereits abgelehnt; als realistische Option bleibt damit nur das BVA, das bereits Aufgaben des BMBF im Bereich der BAföG-Darlehensrückzahlung und im Bereich der Bewilligung des Bildungskredits übernimmt. Dem vorgeschaltet müssten jedoch Gespräche mit BMI geführt werden).

5. MusterVO

Sachsen-Anhalt hat die Kanzlei Redeker mit der Prüfung von datenschutzrechtlichen Fragestellungen sowie mit der Erarbeitung einer Musterverordnung zur Durchführung des elektronischen Verfahrens beauftragt. Der Entwurf der Musterverordnung liegt vor und soll am 21.12.22 nochmals zwischen Sachsen-Anhalt, der Kanzlei sowie BMBF beraten werden. Anschließend soll die Musterverordnung im Länderkreis diskutiert werden. Ein Termin steht hier noch nicht fest, kann aber kurzfristig angesetzt werden.