Dokumentation

Benutzerauthentifizierung über MOA-ID und eIDAS-Infrastruktur

Informationen für Service Provider zur MOA-ID-Release v3.4.0

Version 1.1, 31.07.2018

Thomas Lenz – thomas.lenz@egiz.gv.at
Thomas Zefferer – thomas.zefferer@a-sit.at

Zusammenfassung: MOA-ID Version 3.4.0 unterstützt Benutzerauthentifizierungen basierend auf ausländischen eIDAS-konformen eID-Lösungen. Für Service Provider ergeben sich dadurch potentiell Aspekte, die gesondert betrachtet werden müssen. So sind eine zusätzliche Registrierung der betriebenen MOA-ID-Instanz, sowie ggf. eine Anpassung betriebener Anwendungen notwendig. Um Service Provider beim Upgrade auf die neue MOA-ID-Version und der Integration eIDAS-konformer eID-Lösungen zu unterstützen, fasst dieses Dokument die wesentlichen Aspekte zusammen. Das Dokument fungiert somit als Ergänzung zu den mit der neuen MOA-ID-Release mitgelieferten Release-Notes.

E-Government Innovationszentrum
Inffeldgasse 16/a, A-8010 Graz
Tel. +43 316 873 5514
Fax. +43 316 873 5520
E-Mail post@egiz.gv.at
www.egiz.gv.at

Das E-Government Innovationszentrum ist eine gemeinsame Einrichtung der TU-Graz und des Bundesministeriums für Digitalisierung und Wirtschaftsstandort.

TU Graz

Bundesministerium Digitalisierung und Wirtschaftsstandort

Inhaltsverzeichnis

1 Einleitung 3
2 Architektur und Anmeldeprozess 4
2.1 Herkömmlicher Anmeldeprozess über MOA-ID und Handy-Signatur 4
2.2 Anmeldeprozess über MOA-ID und eID-konforme europäische eID 5
3 Einschränkungen für Service Provider 9
3.1 Keine Unterstützung für privatwirtschaftliche Anwendungen 9
3.2 Keine Unterstützung für qualifizierte Signaturen 9
3.3 Vorerst keine Unterstützung für elektronische Vollmachten 10
3.4 Änderungen in erhaltenen Identity Assertions 10
3.5 Notwendige Registrierung eigener MOA-ID-Instanzen 10
4 Checkliste für Service Provider 11

1 Einleitung

Version 3.4.0 von MOA-ID bietet Service Providern des öffentlichen Sektors eine Unterstützung für eIDAS-basierte Authentifizierungsprozesse von Benutzern. Dadurch wird es möglich, dass sich EU-Bürgerinnen und EU-Bürger mit ihrer landesspezifischen elektronischen eID (z.B. dem deutschen elektronischen Personalausweis) an österreichischen Services des öffentlichen Sektors authentifizieren können.

Aus Sicht der Services erfolgt die Authentifizierung wie bisher über MOA-ID, allerdings erfolgt im Falle einer eIDAS-basierten anstelle der für österreichische Benutzerinnen und Benutzern üblichen Authentifizierung über Bürgerkarte oder Handy-Signatur eine Weiterleitung der Benutzerin bzw. des Benutzers an die eID-Infrastruktur des jeweiligen Heimatlandes. So werden zum Beispiel deutsche Benutzerinnen und Benutzer zur Authentifizierung an eine zentrale Middleware-Komponente weitergeleitet, die die Authentifizierung der Benutzerin bzw. des Benutzers über den deutschen elektronischen Personalausweis vornimmt. Da unabhängig von der Nationalität der Benutzerin bzw. des Benutzers weiterhin MOA-ID als Authentifizierungs-Schnittstelle für das jeweilige Service fungiert, bleibt der Authentifizierungsprozess – ob über Handy-Signatur oder über eine angebundene eIDAS-konforme eID-Komponente eines anderen Landes – für das Service weitgehend transparent.

Allerdings unterscheiden sich die eID-Systeme der diversen europäischen Länder in einigen Details. Daraus ergibt sich erzwungenermaßen, dass MOA-ID seinen angebundenen Services je nach verwendeter Authentifizierungsmethode (Handy-Signatur oder Authentifizierung über eine eIDAS-konforme eID-Lösung) punktuell unterschiedliche Identitätsinformationen der authentifizierten Person liefern kann. Dies kann potentiell Auswirkungen auf Service haben, die in jedem Fall von einer Bereitstellung von Identitätsdaten ausgehen, wie sie im Falle einer Authentifizierung über Bürgerkarte oder Handy-Signatur erfolgt.

Um diesbezügliche Probleme bei der Migration auf MOA-ID Version 3.4.0 und der Verwendung eIDAS-basierter Anmeldeprozesse zu verhindern, beschreibt dieses Dokument in Ergänzung zu den mit der MOA-ID-Release Version 3.4.0 mitgelieferten Release-Notes relevante Aspekte für Service Provider im Detail. Damit soll dieses Dokument Service Provider bei der Integration einer Unterstützung eIDAS-basierter Authentifizierungsprozesse in ihre Services unterstützen.

2 Architektur und Anmeldeprozess

Im Folgenden wird zum besseren Verständnis zunächst ein herkömmlicher Anmeldeprozess über Handy-Signatur skizziert und danach einem eIDAS-basierten Anmeldeprozess gegenübergestellt.

2.1 Herkömmlicher Anmeldeprozess über MOA-ID und Handy-Signatur

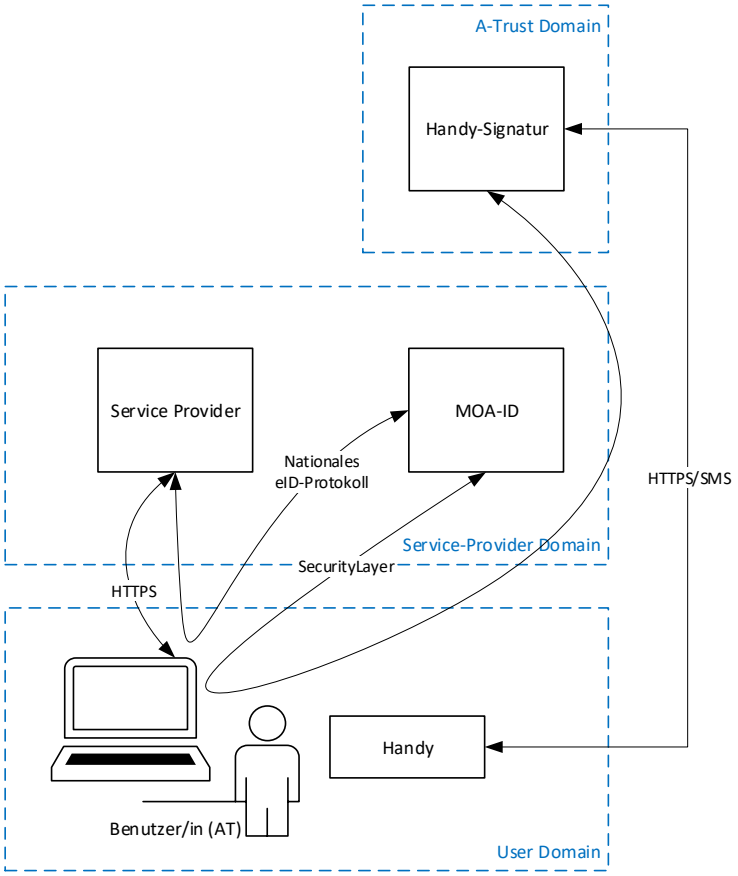

Abbildung 1. Herkömmliche Benutzerauthentifizierung über Handy-Signatur.

Abbildung 1 zeigt involvierte Komponenten eines Authentifizierungsprozesses über Handy-Signatur, wie er bereits bisher von MOA-ID umgesetzt wurde. Dieser gliedert sich grob in folgende Schritte:

1) Die Benutzerin bzw. der Benutzer greifen mit dem Client (Web-Browser) auf einen Dienst des Service Providers zu.
2) Um die Benutzerin bzw. den Benutzer zu authentifizieren, sendet der Service Provider einen Authentifizierungs-Request entsprechend dem nationalen eID-Protokoll an MOA-ID. Dies passiert über den Browser, wodurch dieser an MOA-ID weitergeleitet wird.

3) Der Benutzerin bzw. dem Benutzer wird die Möglichkeit gegeben, zwischen einer Anmeldung über Bürgerkarte oder Handy-Signatur zu wählen. Dieses Beispiel geht davon aus, dass die Option Handy-Signatur gewählt wird.
4) MOA-ID kommuniziert über die SecurityLayer-Schnittstelle mit der Handy-Signatur. Über entsprechende SecurityLayer-Requests fordert MOA-ID unter anderem die Personenbindung der Benutzerin bzw. des Benutzers von der Handy-Signatur an und veranlasst die Erstellung einer qualifizierten Signatur durch die Benutzerin bzw. den Benutzer. Auch in diesem Schritt wird der Browser weitergeleitet (an die Handy-Signatur), sodass notwendige Benutzerinteraktionen direkt mit der Handy-Signatur erfolgen können. So kann eine erste Identifizierung und Authentifizierung der Benutzerin bzw. des Benutzers gegenüber der Handy-Signatur durch Eingabe von Telefonnummer und Passwort im Browser erfolgen. Für die Erstellung der qualifizierten Signatur erfolgt ein zusätzlicher Authentifizierungsschritt über das Handy der Benutzerin bzw. des Benutzers (SMS-TAN oder QR-Code-basierte Authentifizierung).
5) MOA-ID erhält von der Handy-Signatur im Zuge eines Authentifizierungsprozesses die Personenbindung der Benutzerin bzw. des Benutzers (diese enthält das „Minimal Dataset" bestehend aus Vorname, Zuname, Geburtsdatum und Stammzahl), sowie eine qualifizierte Signatur (signierten Auth.-Block) der Benutzerin bzw. des Benutzers. MOA-ID erstellt aus diesen Daten eine Identity-Assertion. Dazu berechnet MOA-ID für Services des öffentlichen Sektors aus der erhaltenen Stammzahl die bPK für den jeweiligen Bereich des Services. Diese enthält dementsprechend das „Minimal Dataset" und den signierten Auth.-Block. Ja nach Konfiguration von MOA-ID enthält die Identity Assertion bei Services des öffentlichen Sektors neben der berechneten bPK auch die Stammzahl der Benutzerin bzw. des Benutzers.
6) Die erstellte Identity Assertion wird an den Service Provider retourniert. Dieser kann die Assertion prüfen und aus ihr die notwendigen Attribute (Vorname, Nachname, Geburtsdatum, bPK, Personenbindung (optional), etc.) extrahieren, um so die Benutzerin bzw. den Benutzer zu authentifizieren. Die erwähnten Attribute liegen in der erhaltenen Identity Assertion an mehreren Stellen vor – so unter anderem auch (aber nicht nur) im signierten Auth.-Block, der in der Assertion enthalten ist.
7) Wurde die Benutzerin bzw. der Benutzer durch Extraktion der von MOA-ID gelieferten Attribute authentifiziert, ist eine erfolgreiche Anmeldung am Service Provider erfolgt.

2.2 Anmeldeprozess über MOA-ID und eID-konforme europäische eID

Die aktuelle Version von MOA-ID unterstützt für Services des öffentlichen Bereichs neben der bisher schon unterstützen und oben rudimentär beschriebenen Benutzerauthentifizierung über Handy-Signatur (oder Bürgerkarte) nun auch eine

Authentifizierung über eIDAS-konforme europäische eIDs. Ziel ist es, die tatsächlich verwendete Benutzerauthentifizierungsmethode (Handy-Signatur oder eIDAS-konforme eID) für den Service Provider so transparent wie möglich zu gestalten. Aufgrund technischer Einschränkungen ergeben sich jedoch bei einer Authentifizierung über eine eIDAS-konforme eID punktuell Unterschiede, die für Service Provider relevant sein können. Um diese zu illustrieren, wird im Folgenden ein typischer Authentifizierungsprozess unter Verwendung des eIDAS-konformen deutschen elektronischen Personalausweises skizziert. Die Grundannahme hinter dem skizzierten Beispiel ist dementsprechend, dass sich eine deutsche Benutzerin bzw. ein deutscher Benutzer mit ihrem bzw. seinem deutschen elektronischen Personalausweis an einem österreichischen Service Provider anmelden möchte.

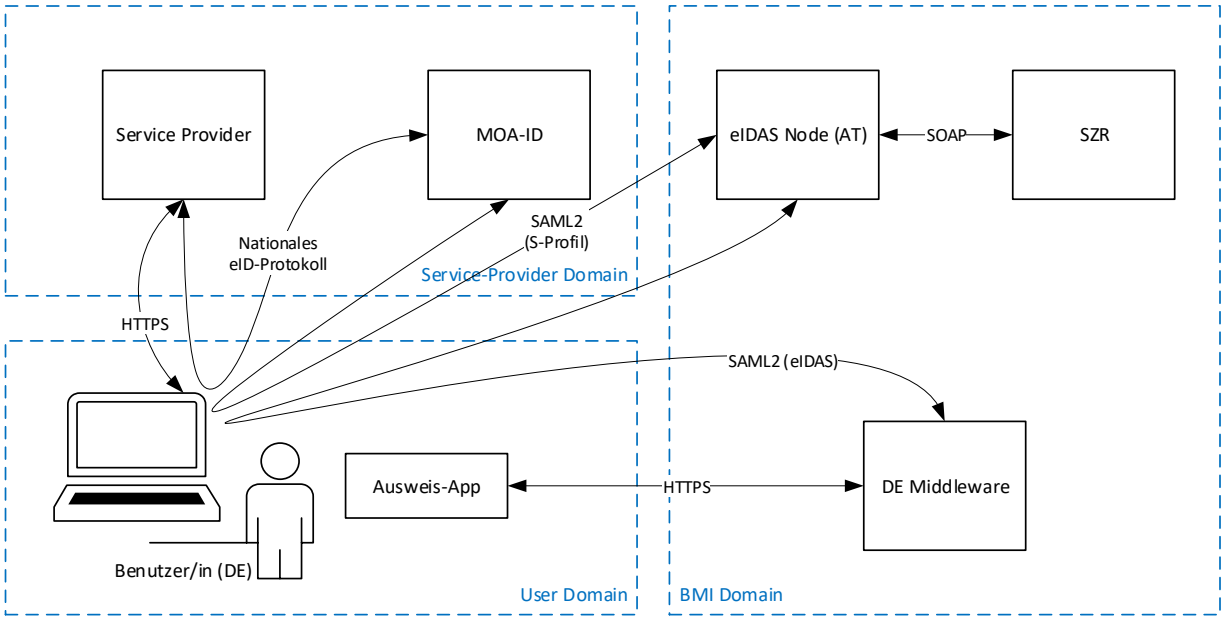

Abbildung 2. eIDAS-basierte Benutzerauthentifizierung (exemplarisch dargestellt für deutsche Benutzerinnen und Benutzer)

Abbildung 2 zeigt involvierte Komponenten eines Authentifizierungsprozesses über den deutschen elektronischen Personalausweis, wie er von MOA-ID Version 3.4.0 nun zusätzlich unterstützt wird. Dieser Authentifizierungsprozess gliedert sich in folgende Schritte:

1) Die Benutzerin bzw. der Benutzer greifen mit dem Client (Web-Browser) auf einen Dienst des Service Providers zu. Dieser Schritt ist äquivalent zu Schritt 1) in Abschnitt 2.1.
2) Um die Benutzerin bzw. den Benutzer zu authentifizieren, sendet der Service Provider einen Authentifizierungs-Request entsprechend dem nationalen eID-

Protokoll an MOA-ID. Dies passiert über den Browser, wodurch dieser an MOA-ID weitergeleitet wird. Dieser Schritt ist äquivalent zu Schritt 2) in Abschnitt 2.1.

3) Der Benutzerin bzw. dem Benutzer wird die Möglichkeit gegeben, zwischen einer Anmeldung über Bürgerkarte oder Handy-Signatur zu wählen. Zusätzlich wird die Option „EU Login“ angezeigt. Dieses Beispiel geht davon aus, dass die Option „EU Login“ gewählt wird.
4) MOA-ID sendet einen Authentifizierungs-Request an die zentrale österreichische eIDAS-Node (AT). Diese wir vom Bundesministerium für Inneres (BMI) betrieben. Die Übermittlung des Requests erfolgt entsprechend dem Protokoll SAML2 (S-Profil) und wird über den Browser der Benutzerin bzw. des Benutzers umgesetzt. Dadurch erfolgt eine Weiterleitung des Browsers an die eIDAS-Node (AT).
5) Die eIDAS-Node (AT) stellt einen Auswahl-Dialog zur Verfügung, über den die Benutzerin bzw. der Benutzer sein Heimatland auswählen kann. Es wird in diesem Beispiel von der Auswahl „Deutschland“ ausgegangen.
6) Entsprechend der getätigten Länderauswahl („Deutschland“) sendet die eIDAS-Node (AT) einen Authentifizierungs-Request an eine Middleware-Komponente der deutschen eID-Infrastruktur (DE Middleware). Diese wird zusammen mit der eIDAS-Node (AT) ebenfalls vom BMI betrieben. Die Übermittlung des Authentifizierungs-Requests folgt dem SAML2-basierten eIDAS-Protokoll. Technisch erfolgt die Übermittlung über den Browser der Benutzerin bzw. des Benutzers, wodurch dieser an die DE Middleware weitergeleitet wird.
7) Die DE Middleware authentifiziert die Benutzerin bzw. den Benutzer über den deutschen elektronischen Personalausweis. Dazu kommuniziert die DE Middleware mit der Ausweis-App am System der Benutzerin bzw. des Benutzers. Aus dem Personalausweis wird im Zuge des Authentifizierungsvorgangs das „Minimal Dataset“ ausgelesen. Dieses enthält Vor- und Zunamen, Geburtsdatum und einen Identifier (eID) der Benutzerin bzw. des Benutzers.
8) Das „Minimal Dataset“ wird von der Ausweis-App an die DE Middleware übertragen.
9) Die DE Middleware retourniert das „Minimal Dataset“ entsprechend dem eIDAS-Protokoll an die eIDAS-Node (AT).
10) Die eIDAS-Node (AT) veranlasst im SZR eine Eintragung der Benutzerin bzw. des Benutzers im Ergänzungsregister für natürliche Personen. Im Zuge dessen wird vom SZR auch eine Personenbindung für die Benutzerin bzw. den Benutzer erstellt und an die eIDAS-Node (AT) retourniert. Diese Personenbindung enthält die Stammzahl der Benutzerin bzw. des Benutzers.
11) MOA-ID erstellt basierend auf den erhaltenen Daten („Minimal Dataset“, sowie Personenbindung mit Stammzahl) eine Identity Assertion. Wenn notwendig, berechnet MOA-ID dazu aus der erhaltenen Stammzahl das entsprechende bPK. Die erstellte Identity Assertion wird an den Service Provider retourniert. Dieser kann

die Assertion prüfen und aus ihr die notwendigen Attribute (Vorname, Nachname, Geburtsdatum, bPK, Personenbindung) extrahieren, um so die Benutzerin bzw. den Benutzer zu authentifizieren.

12) Wurde die Benutzerin bzw. der Benutzer durch Extraktion der von MOA-ID gelieferten Attribute authentifiziert, ist eine erfolgreiche Anmeldung am Service Provider erfolgt.

3 Einschränkungen für Service Provider

Aus der in Abschnitt 2 erfolgten Gegenüberstellung der Authentifizierungsprozesse über Handy-Signatur bzw. über eine eIDAS-konforme ausländische eID ist ersichtlich, dass die Wahl des Authentifizierungsprozesses für den Service Provider weitgehend transparent ist. Dies ist vergleichbar mit der bisher schon möglichen Auswahl zwischen Handy-Signatur und Bürgerkarte, welche auf die Funktionalität des Service Providers ebenfalls kaum Auswirkungen hatte.

In vielen Punkten gilt dies nun auch für Authentifizierungsprozesse über eIDAS-konforme ausländische eIDs. Weiterhin fungiert MOA-ID als einzige Schnittstelle für den jeweiligen Service Provider, an die Authentifizierungs-Requests gesendet werden können. Unabhängig vom durch MOA-ID durchgeführten Authentifizierungsprozess (Handy-Signatur, Bürgerkarte, eIDAS-konforme eID) liefert MOA-ID am Ende eine Identity Assertion an den Service Provider aus, über die dieser die Benutzerin bzw. den Benutzer authentifizieren kann.

Durch technische Unterschiede zwischen der österreichischen eID-Lösung (Handy-Signatur bzw. Bürgerkarte) und ausländischen eIDAS-konformen eID-Lösungen ergeben sich trotz der weitgehend übereinstimmenden Authentifizierungsprozesse punktuell Unterschiede, die von Service Providern bzw. den von ihnen betriebenen Services berücksichtigt werden müssen. Diese sind im Folgenden angeführt.

3.1 Keine Unterstützung für privatwirtschaftliche Anwendungen

Aufgrund der rechtlichen Situation unterstützt die aktuelle Umsetzung der österreichischen eIDAS-Node (AT) derzeit noch keine Auslieferung von Personenbindungen mit wbPK. Dementsprechend können Service Provider des privatwirtschaftlichen Bereichs, an welche keine Personenbindungen mit Stammzahl ausgeliefert werden dürfen, die Authentifizierungsmethode über eIDAS-konforme europäische eIDs noch nicht nutzen.

3.2 Keine Unterstützung für qualifizierte Signaturen

Es sei darauf hingewiesen, dass bei Zulassen von Benutzerauthentifizierungen über eine eIDAS-konforme eID nicht mehr davon ausgegangen werden kann, dass die Benutzerin bzw. der Benutzer in der Lage sind, eine qualifizierte elektronische Signatur zu erstellen. Dies kann speziell für jene Service Provider relevant sein, die nach erfolgter Anmeldung im Zuge des implementierten Verfahrens eine qualifizierte Signatur (z.B. zum Signieren eines Formulars) verlangen.

3.3 Vorerst keine Unterstützung für elektronische Vollmachten

MOA-ID bietet bei Verwendung von Handy-Signatur und Bürgerkarte Endanwendern die Möglichkeit, sich unter Verwendung des elektronischen Vollmachten-Systems im Namen anderer Personen anzumelden und im Namen dieser Personen Verfahren durchzuführen. Das ausländische eIDAS-basierte eID-Systeme nicht in das österreichische elektronische Vollmachten-System integriert sind, wird bei Verwendung einer eIDAS-basierten eID (z.B. deutscher elektronischer Personalausweis) eine Anmeldung in Vertretung einer anderen Person nicht unterstützt. Bei Verwendung einer eIDAs-basierten eID können sich Benutzerinnen und Benutzer daher an Services vorerst nur in ihrem eigenen Namen anmelden. Eine diesbezügliche Erweiterung der Funktionalität ist für die Zukunft geplant.

3.4 Änderungen in erhaltenen Identity Assertions

Im Zuge eines Authentifizierungsprozesses ermittelte Identitätsinformationen („Minimal Dataset" bPK, etc.) werden dem Service Provider von MOA-ID in Form einer Identity Assertion bereitgestellt. Da sich eIDAS-konforme ausländische eID-Lösungen in einigen Punkten von den österreichischen Lösungen Handy-Signatur und Bürgerkarte unterscheiden, ergeben sich zwangsweise auch Unterschiede im Format der von MOA-ID bereitgestellten Identity Assertion. Konkret ergeben sich bei Authentifizierung über eine eIDAS-konforme ausländische eID-Lösung Einschränkungen. So enthält die erhaltene Identity Assertion keinen von der Benutzerin bzw. dem Benutzer signierten Auth.-Block und dementsprechend auch kein Signaturzertifikat der Benutzerin bzw. des Benutzers. Grund ist die fehlende Unterstützung für qualifizierte elektronische Signaturen im eIDAS-Protokoll. Im Zuge des Authentifizierungsprozesses kann daher – anders als bei Handy-Signatur oder Bürgerkarte – keine qualifizierte Signatur von der Benutzerin bzw. vom Benutzer verlangt werden. Für Service Provider bedeutet dies, dass sie benötigte Identitätsdaten nicht aus dem signierten Auth.-Block oder dem inkludierten Signaturzertifikat extrahieren können. Allerdings liegen Identitätsdaten an anderer Stelle der Identity Assertion vor und können von dort extrahiert werden.

3.5 Notwendige Registrierung eigener MOA-ID-Instanzen

Um Authentifizierungs-Requests an die vom BMI betriebene eIDAS-Node (AT) senden zu können, muss die sendende MOA-ID-Instanz vorab beim BMI registriert werden. Ein entsprechender Prozess dafür wird beim BMI implementiert.

4 Checkliste für Service Provider

Unter Berücksichtigung der im vorigen Abschnitt beschrieben Einschränkungen, die sich bei einer Unterstützung eIDAS-konformer ausländischer eID-Lösungen und derer Integration über die aktuelle Version von MOA-ID ergeben, ergibt sich für Service Provider folgende Checkliste.

- **Vorbereitung:** Installation von bzw. Update auf MOA-ID Version 3.4.0 entsprechend den mitgelieferten Release Notes.
- **Registrierung:** Registrierung der MOA-ID-Instanz beim BMI.
- **Kompatibilitätscheck:** Überprüfung der Kompatibilität eigener Anwendungen zu eIDAS-basierten Anmeldeprozessen
    - Verlangen eigene Verfahren eine qualifizierte Signatur von Benutzerinnen und Benutzern?
    - Können eigene Anwendungen mit reduzierten Identity Assertions, wie sie im Falle einer Authentifizierung über eine eIDAS-konforme ausländische eID-Lösung von MOA-ID ausgeliefert werden, umgehen (fehlender signierter Auth.-Block, etc.)?
- **Anpassung des Bürgerkartenumgebungs-/eID-Auswahl-Templates:** Für den Fall, dass von der Anwendung ein eigenes Auswahl-Template bereitgestellt wird, über das Benutzerinnen und Benutzer bisher schon zwischen Handy-Signatur und Bürgerkarte wählen konnten, muss dieses Template um die Option „Login mit eIDAS-basierter eID“ erweitert werden.
- **Testen:** Erste Tests können gegen eine Test-Instanz der eIDAS-Node (AT), die unter https://vidp.gv.at/ms_connector zur Verfügung steht, durchgeführt werden. Bei Interesse kann eine Anfrage gerne an post@egiz.gv.at gestellt werden.

Dokumentenhistorie

Version	Datum	Autor(en)	Anmerkung
0.1	10.07.2018	Thomas Zefferer	Erstentwurf
0.2	12.07.2018	Thomas Lenz	Kommentare
0.3	13.07.2018	Thomas Zefferer	Ergänzungen und Konsolidierung
1.0	25.07.2018	Thomas Zefferer	Abstimmung und Finalisierung der Erstversion
1.1	31.07.2018	Thomas Zefferer	Präzisierung zu privatwirtschaftlichen Service Providern