



**AOV - Agentur für die Verfahren und die Aufsicht im  
Bereich öffentliche Bau-, Dienstleistungs- und  
Lieferaufträge**

**E-proc. 4 - Bereitstellung und Verwaltung der  
telematischen Plattform "Informationssystem Öffentliche  
Verträge" in SaaS-Modalität**

**An\_3.17\_Zugangsberechtigungen**

**ACP - Agenzia per i procedimenti e la vigilanza in materia  
di contratti pubblici di lavori, servizi e forniture**

**e-proc4 – Servizio di fornitura e gestione in modalità SaaS  
della piattaforma telematica "Sistema Informativo  
Contratti Pubblici"**

**All\_3.17\_Accreditamenti**

## Zugangsberechtigungen

### Vorgesehene Zugriffsmethoden

Die Plattform bietet derzeit den Zugang mittels Benutzername und Passwort. Diese Anmeldedaten identifizieren die Benutzerinnen und die Art des Subjekts, wofür sie arbeiten:

Es gibt zwei Arten von Subjekten:

- Nutzer von Vergabestellen / Kostenstellen
- Wirtschaftsteilnehmer

Nach der Verleihung der Zugangsberechtigung erhalten Benutzerinnen die Ihnen zugewiesenen Profile und Rollen.

### Die gesetzliche Verpflichtung

Die Plattform muss in der Lage sein, Benutzerinnen gemäß dem Artikel 3 des Ministerialdekrets 148/2021 zu authentifizieren, indem sie innerhalb von sechs Monaten nach dem Inkrafttreten der von Agid herausgegebenen Leitlinien gemäß dem Artikel 29 des Ministerialdekrets 148/2021 angepasst wird.

Je nach geografischer Herkunft der Nutzer (national, EU, Nicht-EU) müssen unterschiedliche Zugriffsmethoden vorgesehen werden:

- Nationale Nutzer: Die Zugriffsmethoden sind SPID/CIE/CNS.
- EU-Nutzer: Die Quelle dafür ist die EIDAS-Verordnung und die entsprechenden Durchführungsbestimmungen. Für Wirtschaftsteilnehmer aus Nicht-EU-Ländern, die nicht Mitglied von EIDAS sind, muss der Zugang mittels Benutzername+Passwort gewährt werden.
- Nicht-EU-Nutzer: Die Authentifizierung erfolgt über Benutzernamen und Passwort.

Für die Aktivierung der SPID/CIE/CNS- und EIDAS-Authentifizierung muss eine Übergangsphase vorgesehen werden, in der der Zugriff auf die ISOV Plattform sowohl mit den oben genannten Methoden als auch mit Benutzername und Passwort möglich ist.

### Die Implementierung auf der ISOV-Plattform

Der Administrator erteilt der Bezugsperson der Kostenstelle die Zugangsberechtigungen. Weitere interne Zugangsberechtigungen werden von der Bezugsperson der Kostenstelle verwaltet. Diese muss nämlich in der Lage sein, weitere interne Benutzer aus der Benutzer Liste auszuwählen und diesen unterschiedliche Berechtigungen zuzuweisen. Die ISOV-Plattform muss über ein Berechtigungssystem verfügen, das die Verwaltung der mit den Rollen oder bestimmten Nutzern verbundenen Berechtigungen für jedes Modul gemäß dem Anhang 3.3 zu Rollen und Profilen ermöglicht. Die

Zugänglichkeit muss daher je nach den Nutzerinnen zugewiesenen Privilegien selektiv gewährleistet werden. Eine ähnliche Verwaltung muss für die Wirtschaftsteilnehmer vorgesehen werden.

Um auf die ISOV-Plattform zuzugreifen, wird den Nutzerinnen ein neuer Bereich auf der Hauptseite in der Nähe des traditionellen Anmeldebereichs zur Verfügung gestellt, der die Zugangsmodalitäten gemäß Art. 3 DM 148/2021 enthält. Beim Zugriff auf diese Funktion werden die Nutzerinnen auf die Anmeldeseite von myCIVIS (Diensteanbieter) weitergeleitet, wo sie einen der verfügbaren Authentifizierungsmethoden (SPID/CIE/CNS/EIDAS) auswählen können.

Bei der SPID-Akkreditierung überprüft MyCIVIS die Identität der Nutzerinnen über einen Identitätsanbieter (PosteID, Infocert, Lepida, Tim, Namiral usw.) und sendet im Falle einer positiven Überprüfung die Steuernummer und einige Informationen über die zugriffsberechtigten Nutzerinnen an die ISOV-Plattform zurück. Die ISOV-Plattform identifiziert die Nutzerinnen anhand deren Steuernummer und prüft, für welche Subjekte sie tätig werden können. Anhand der Steuernummer stellt die Plattform fest, ob den NutzerInnen mehrere Rollen zugeordnet sind. Wenn die Rolle der Nutzerinnen eindeutig sind, haben sie direkten Zugriff auf den reservierten Bereich der ISOV-Plattform und können im Namen des identifizierten Subjekts arbeiten. Sollten jedoch mehrere Zugangsberechtigungen mit derselben Steuernummer verbunden sein, werden die Nutzerinnen aufgefordert, die Berechtigung und das Subjekt auszuwählen, wofür sie arbeiten möchten (z.B. Wirtschaftsteilnehmer, Vergabestelle, Kostenstelle usw.), bevor sie in den reservierten Bereich der ISOV-Plattform einsteigen können.

Nach dem Einloggen muss die Plattform es den Nutzerinnen ermöglichen, in derselben Sitzung zu einer der mit ihren Steuernummern verbundenen Zugangsberechtigungen zu wechseln.

Alle Zugangsvorgänge, sowohl die mit Benutzername und Passwort als auch die mit SPID/CNS/CIE/EIDAS, sowie alle vom Diensteanbieter bereitgestellten Token müssen erfasst werden, um eine Gegenprüfung zu ermöglichen.

Die ISOV-Plattform muss vierundzwanzig Monate lang die Informationen aufbewahren, die erforderlich sind, um die in seinen Systemen über SPID durchgeführten Aktionen den einzelnen digitalen Identitäten zuzuordnen (Artikel 13, Absatz 2 des Dekrets des Ministerpräsidenten vom 24. Oktober 2014). Diese Aufzeichnungen bilden das Transaktionsregister des Diensteanbieters.

Bezüglich der Authentifizierung über EIDAS, da es sich um Nutzerinnen aus dem Ausland handelt, gibt es keinen zwischen den Staaten geteilten eindeutigen Code, der sie identifiziert, und daher werden nach Abschluss des Authentifizierungsprozesses nur der Nachname und Vorname als Metadaten zurückgesendet. Die ISOV-Plattform muss die Identifizierung der Zugangsberechtigungen mittels Nachname und Name durchführen.