Lieferantenstammdatenverwaltung (SMDM) Lieferanten-Zugangsberechtigung

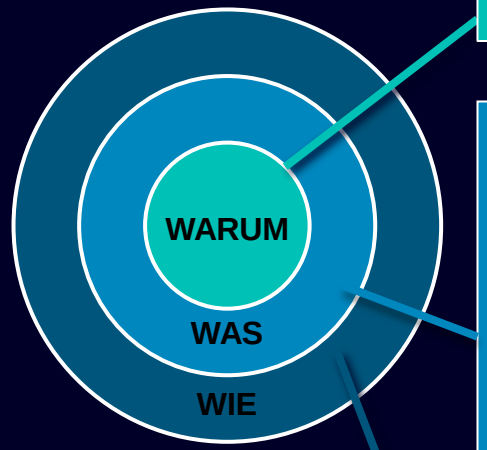
Lieferantenportal

SIEMENS

Lieferantenstammdatenverwaltung (SMDM)
Inhalt

SIEMENS

Lieferanten-Zugangsberechtigung
Hintergrund, Zielsetzung, Vorgehensweise



Anforderungen an die Informationssicherheit zum Schutz vor Cyberangriffen durch externe Benutzer machen einen sicheren Anmeldemechanismus erforderlich.

Supplier Entitlement ist ein Zugangssystem für Lieferanten, um über eine einzigartige 2-Faktor-Authentifizierung Zugriff auf Siemens-Anwendungen zu erhalten:

- Faktor 1: Berechtigungs-E-Mail-Adresse + Passwort
- Faktor 2: Ein zusätzlicher Faktor, der dem jeweiligen Benutzer zur Verfügung gestellt wird

Basierend auf der ausgewählten zweiten Authentifizierungsmethode erhalten Lieferanten

- Option 1: eine Push-Benachrichtigung auf dem Mobiltelefon (Guardian-App)
- Option 2: Ein Einmalpasswort (OTP) per Textnachricht (SMS) auf dem Mobiltelefon
- Option 3: Einen Code, der nach dem Scannen des QR-Codes über die Authentifizierungs-App generiert wird

Nach erfolgreicher Bestätigung wird der Anwendungszugriff gewährt.

SIEMENS

Lieferantenstammdatenverwaltung (SMDM)
Inhalt

SIEMENS

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

SIEMENS

October 10, 2023

Lieferantenregistrierung

Diese E-Mail wird automatisch generiert. Bitte antworten Sie nicht auf diese E-Mail-Adresse.

Sehr geehrter Lieferant,

mit dieser E-Mail möchten wir Sie darüber informieren, dass Siemens Ihr Unternehmen auf seinem Lieferantenportal SCM STAR registriert hat, um so in Zukunft geschäftliche Aktivitäten mit Ihnen durchführen zu können.

Um bei Siemens den Status "Ready for Business" zu erhalten und damit für Bestellungen, Ausschreibungen und Verträge qualifiziert zu sein, bitten wir Sie, den Hinweisen in dieser Email zu folgen und den beigefügten Antrag zeitnah (innerhalb der nächsten 2 Tage) zu vervollständigen. Vielen Dank für Ihr Verständnis und Ihre Zuarbeit.

Bitte klicken Sie hier , um den Antrag zu vervollständigen.

Loggen Sie sich zum ersten Mal ein?
Wie Sie sich in wenigen Schritten einloggen können, erfahren Sie in diesem Video oder in dieser Benutzeranleitung. Sie müssen ein gesichertes Single-Sign-On-Konto erstellt haben, um diesen Antrag abzuschließen. Dies ist ein einmaliger Vorgang zum Erstellen einer geschützten Benutzerverbindung im Siemens Authentifizierungsservice. Wenn Sie noch kein aktives Benutzerkonto haben, werden Sie auf die Siemens Authentifizierungsseiten weitergeleitet. Nachdem Sie Ihr Benutzerkonto aktiviert haben, werden Sie zu dem Lieferantenstammdatenantrag weitergeleitet.

Fragen?

- Email: s2c_support.scm@siemens.com
- Internetseiten für Lieferanten (beinhaltet User Guides im Download Center): http://www.siemens.com/supplierportal

Siemens AG / Supply Chain Management
(Betreiber von SCM STAR für alle teilnehmenden Gesellschaften)

siemens.com Global Website Restricted © Siemens AG, 2023

A

Bitte klicken Sie hier , um den Antrag zu vervollständigen.

B

Loggen Sie sich zum ersten Mal ein?
Wie Sie sich in wenigen Schritten einloggen können, erfahren Sie in diesem Video oder in dieser Benutzeranleitung. Sie müssen ein gesichertes Single-Sign-On-Konto erstellt haben, um diesen Antrag abzuschließen. Dies ist ein einmaliger Vorgang zum Erstellen einer geschützten Benutzerverbindung im Siemens Authentifizierungsservice. Wenn Sie noch kein aktives Benutzerkonto haben, werden Sie auf die Siemens Authentifizierungsseiten weitergeleitet. Nachdem Sie Ihr Benutzerkonto aktiviert haben, werden Sie zu dem Lieferantenstammdatenantrag weitergeleitet.

C

Fragen?

- Email: s2c_support.scm@siemens.com
- Internetseiten für Lieferanten (beinhaltet User Guides im Download Center): http://www.siemens.com/supplierportal

Sie erhalten eine Benachrichtigungs-E-Mail von star.scm@siemens.com mit einem Aktivierungslink – bitte klicken Sie auf Link (A), um zum Aktivierungsprozess der Multi-Faktor-Authentifizierung weitergeleitet zu werden. Als unterstützendes Material können Sie eine Videoanleitung oder ein Benutzerhandbuch (B) verwenden. Bei Fragen wenden Sie sich bitte an das Support-Team, E-Mail-Kontakt: s2c_support.scm@siemens.com. Dokumente können im Supplier Portal über das Download Center (C) eingesehen werden.

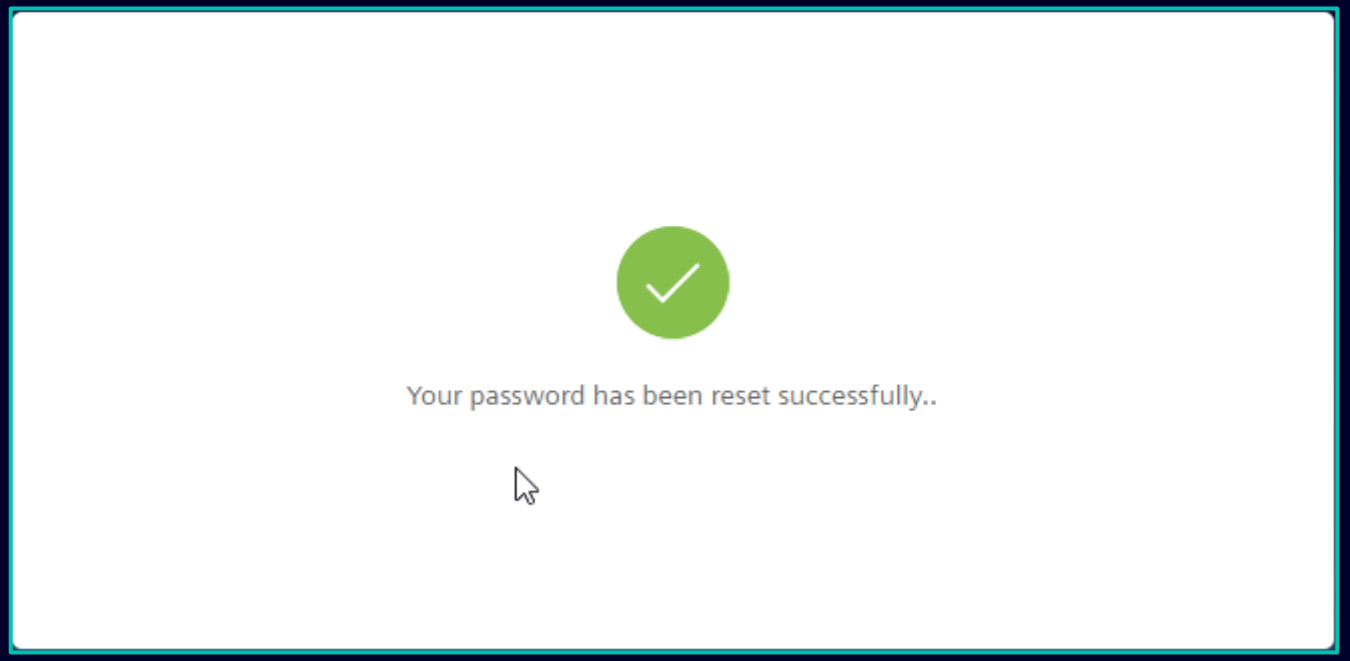
SIEMENS

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

Nachdem Sie auf den Initiierung Link geklickt haben, werden Sie zur Siemens-Login-Webseite weitergeleitet. Richten Sie zunächst ein sicheres Passwort ein, das auf den Passwortrichtlinien basiert. Sobald Sie Ihr Passwort eingegeben haben, klicken Sie auf „Reset Password“.

SIEMENS

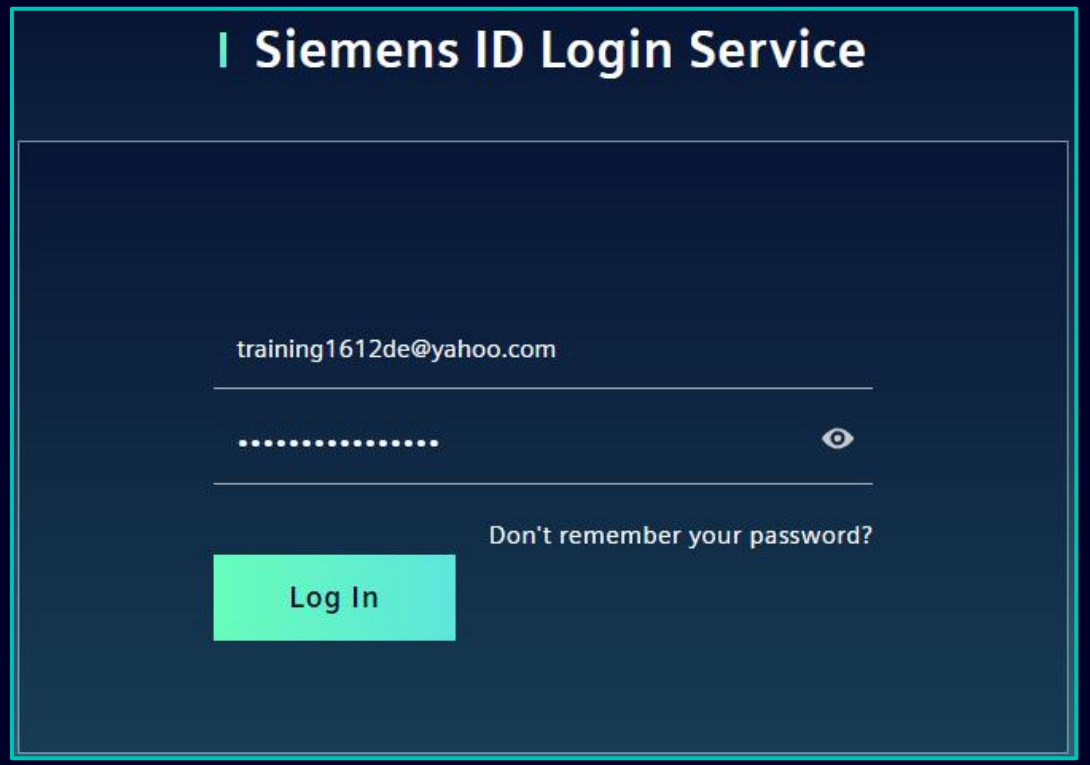
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung



Nach dem Zurücksetzen Ihres Passworts wird eine Bestätigungsmeldung angezeigt und Sie werden zur Anmeldung mit Ihrem neu festgelegten Passwort weitergeleitet.

SIEMENS

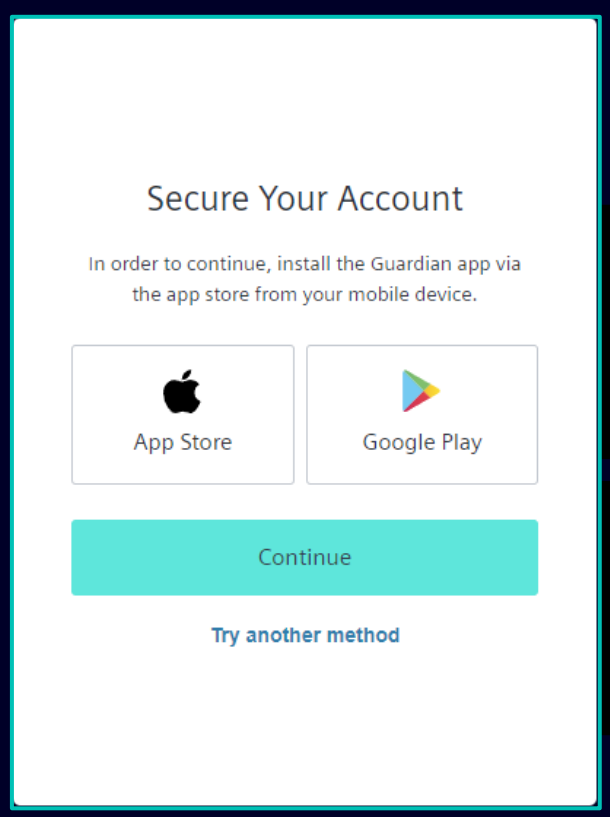
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

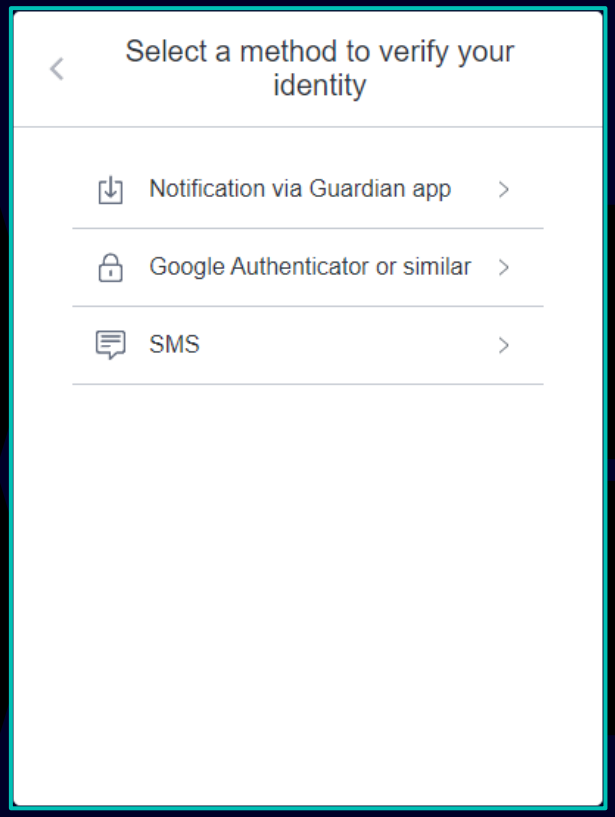


Falls Sie Ihr neues Passwort vergessen haben, klicken Sie bitte auf „Don‘t remember your password?“ und hier weitermachen.

SIEMENS

Erste Aktivierung der Multi-Faktor-Authentifizierung
Wählen Sie Ihre bevorzugte zweite Authentifizierungsmethode





Wählen Sie eine der folgenden Apps:

Guardian app for Android and Apple IOS

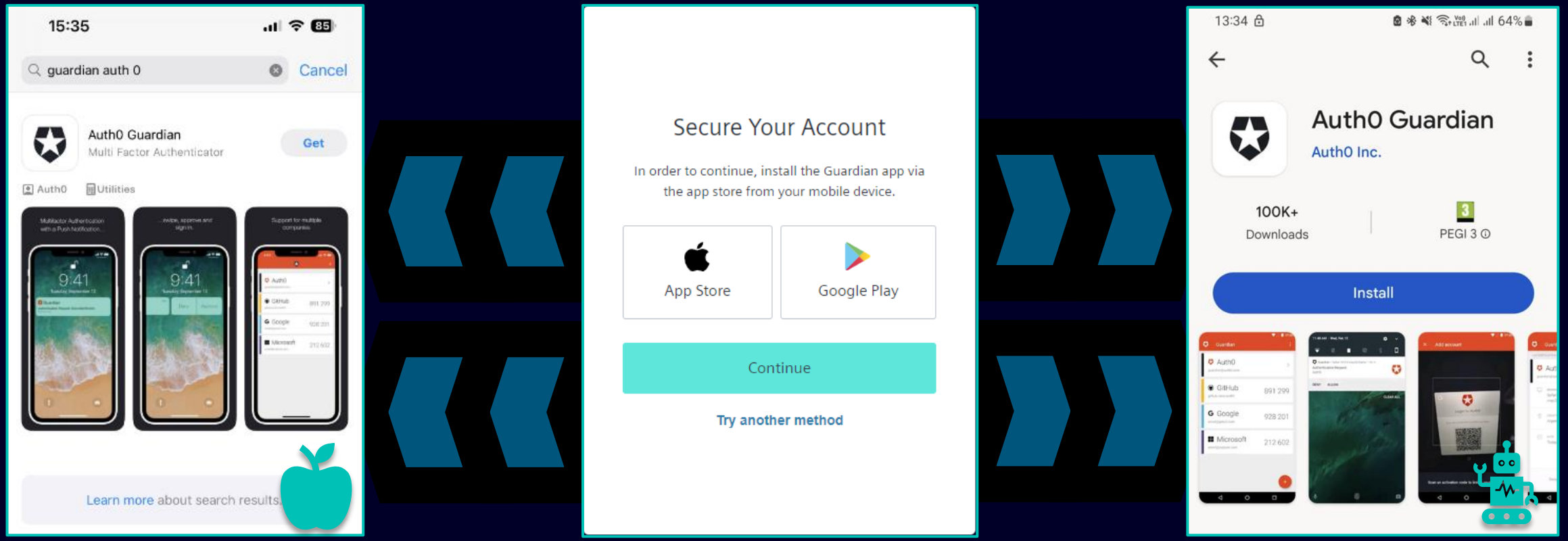
Google Authenticator or similar app

Google Authenticator or similar app

Nachdem Sie Ihr Passwort festgelegt haben, werden Sie weitergeleitet, um die zweite Authentifizierungsmethode auszuwählen. Sie können zwischen der Guardian-App, dem Google Authenticator oder einer ähnlichen App und der Authentifizierung der Mobiltelefonnummer wählen. Bitte wählen Sie Ihre bevorzugte zweite Authentifizierungsmethode aus und verwenden die Links für Guardian app for Android and Apple IOS, Google Authenticator or similar app, mobile phone number authentication.

SIEMENS

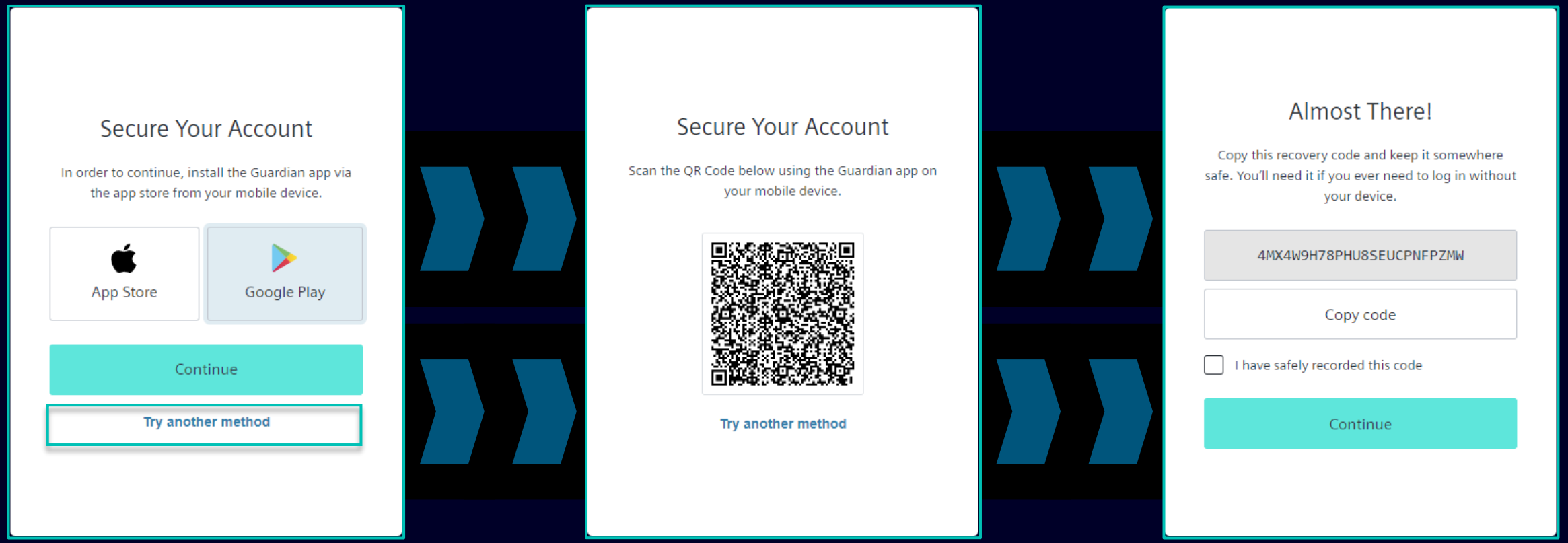
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Guardian-App für Android und Apple IOS



Wenn Sie Ihr Android- oder Apple IOS-Gerät für die zweite Authentifizierungsmethode verwenden möchten, sollten Sie die **Guardian-App** auswählen. Sie können den direkten Link verwenden, indem Sie auf das Google Play-Symbol oder das App Store-Symbol klicken. Suchen Sie auf Ihrem Mobiltelefon/Tablet nach der App „Auth0 Guardian“. Fahren Sie nach erfolgreicher Installation der App mit dem nächsten Schritt fort.

SIEMENS

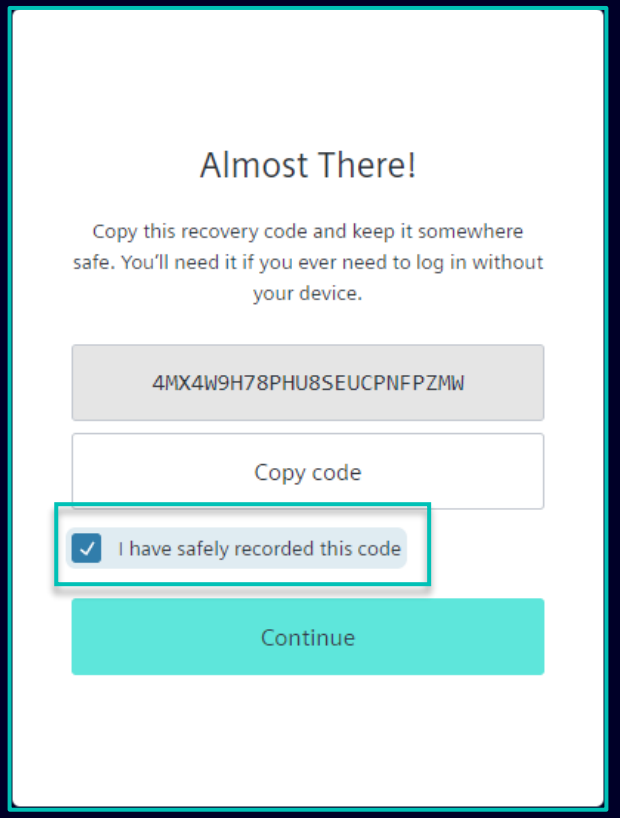
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Guardian-App für Android und Apple IOS



Sobald die Guardian-App erfolgreich auf Ihrem Andorid-Gerät installiert wurde, wählen Sie „Continue“. Es wird ein eindeutiger QR-Code generiert. Öffnen Sie die Guardian-App auf Ihrem Mobiltelefon/Tablet und scannen Sie den QR-Code. Sobald der QR-Code gescannt wurde, werden Sie aufgefordert, diesen-entweder zu bestätigen oder einen sicheren Satz in der Guardian-App zu erstellen. Im Siemens Login werden Sie aufgefordert, den Wiederherstellungscode zu hinterlegen.

SIEMENS

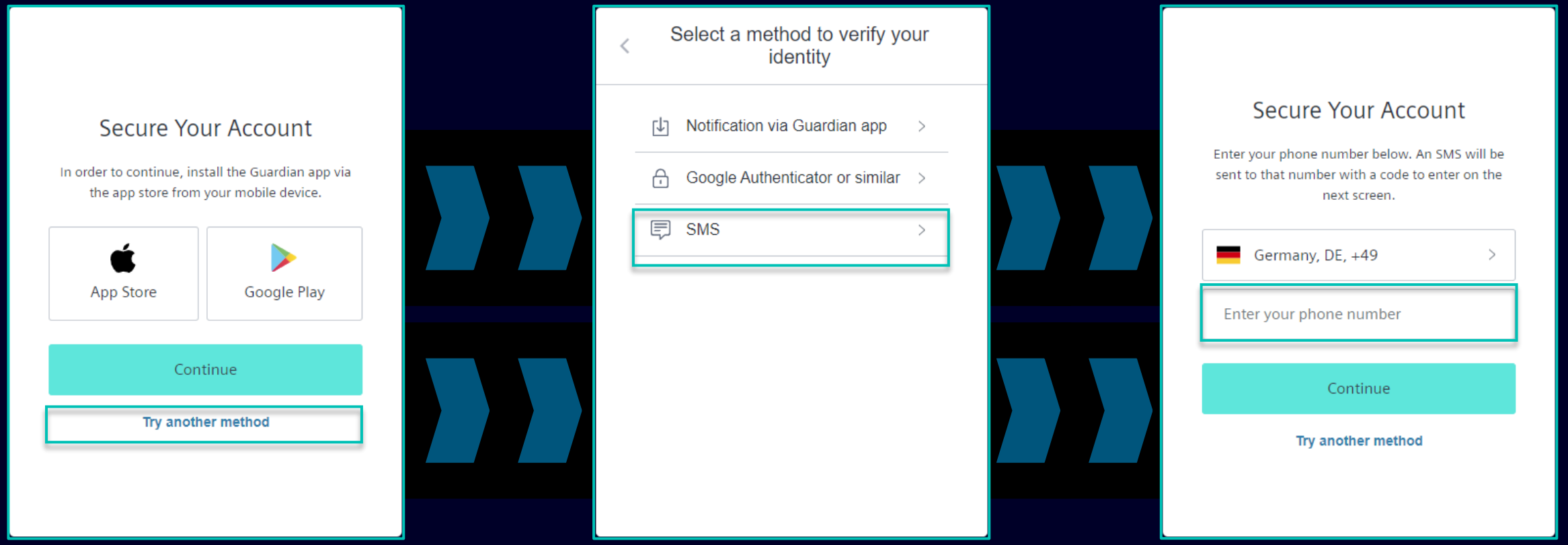
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Guardian-App für Android und Apple IOS



Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie „Continue“. Nachdem Sie auf „Continue“ geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts (wie hier im Beispiel) die Guardian-App automatisch als standardmäßige zweite Authentifizierungsmethode festgelegt.

SIEMENS

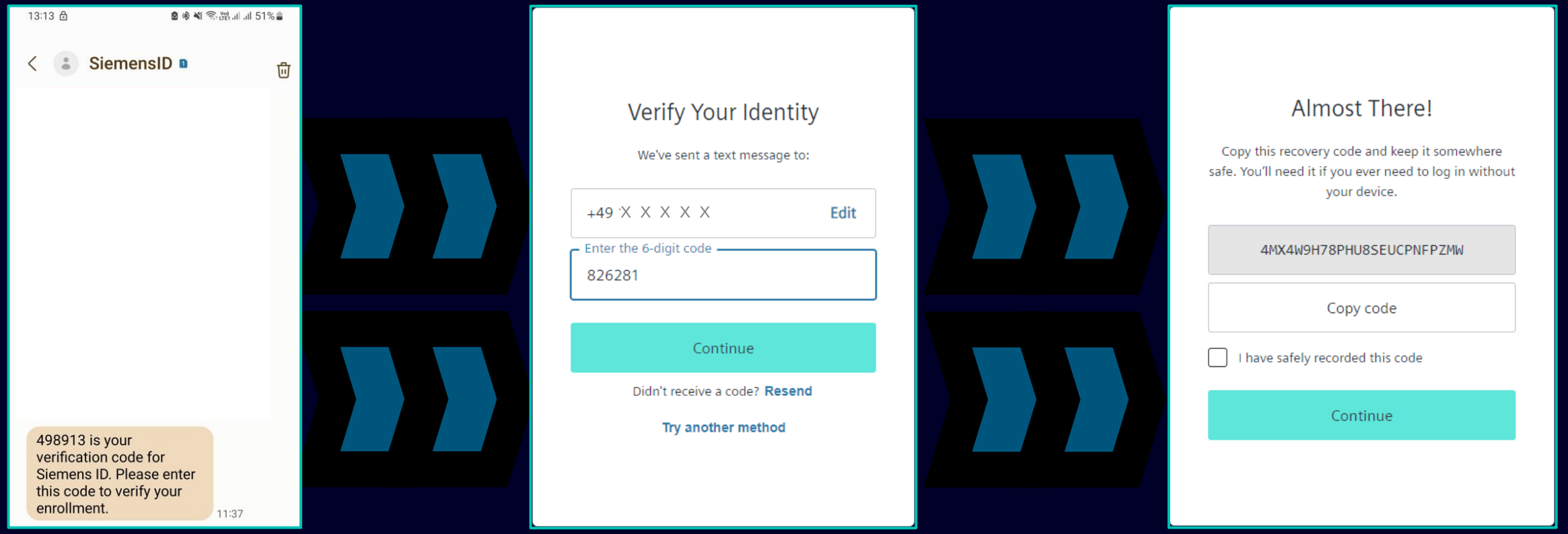
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Authentifizierung der Mobiltelefonnummer



Für die Authentifizierung der Mobiltelefonnummer (SMS-Code) wählen Sie bitte „Try another method “ und dann „SMS“. Wählen Sie die Vorwahl Ihres Landes und geben Sie Ihre Mobilfunknummer (ohne „0“ am Anfang) ein.

SIEMENS

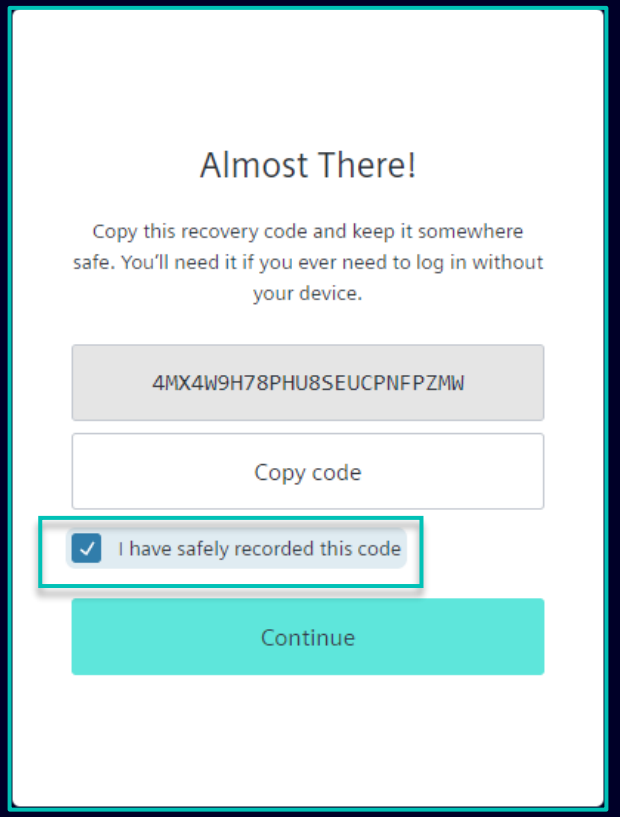
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Authentifizierung der Mobiltelefonnummer



Nach Eingabe Ihrer Mobilfunknummer erhalten Sie eine SMS mit einem 6-stelligen Code. Klicken Sie nach Eingabe des erhaltenen Codes auf „Continue“. Falls Sie den Code nicht erhalten haben, klicken Sie bitte auf „Erneut senden“. Nach erfolgreicher Validierung des 6-stelligen Codes werden Sie aufgefordert, den Wiederherstellungscode zu speichern.

SIEMENS

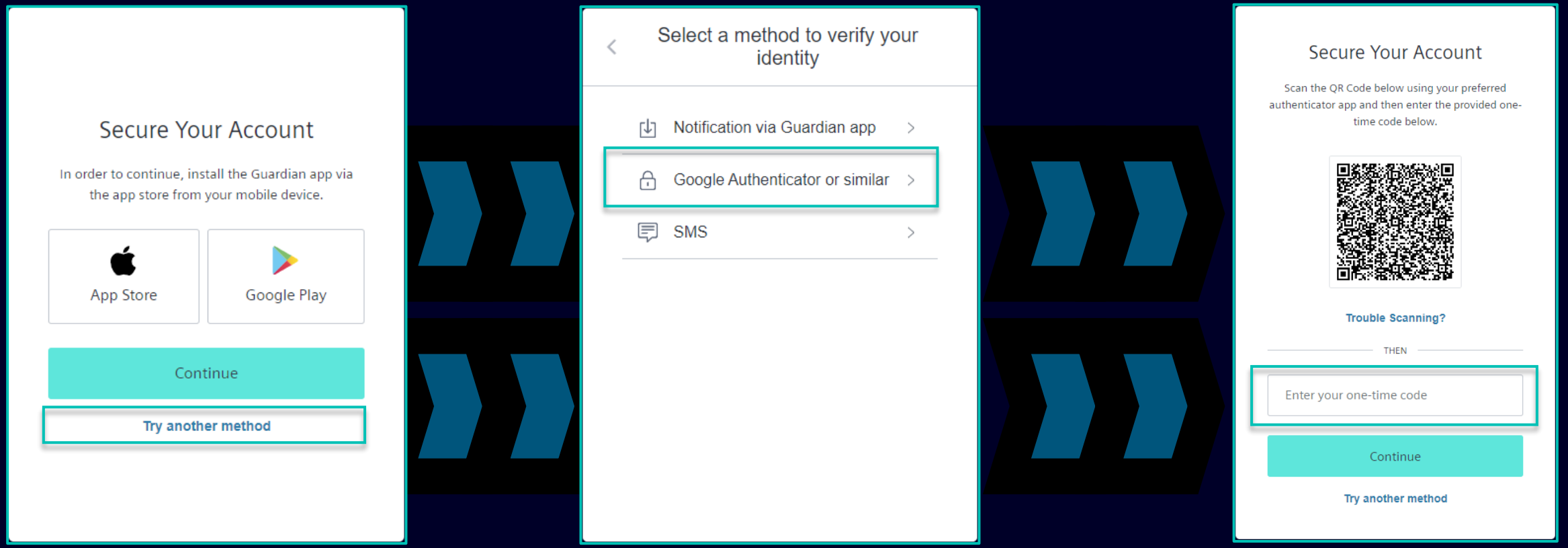
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Authentifizierung der Mobiltelefonnummer



Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie „Continue“. Nachdem Sie auf „Continue“ geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts (wie hier im Beispiel) die SMS-Authentifizierung automatisch als standardmäßige zweite Authentifizierungsmethode festgelegt.

SIEMENS

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung
Google Authenticator oder ähnliches



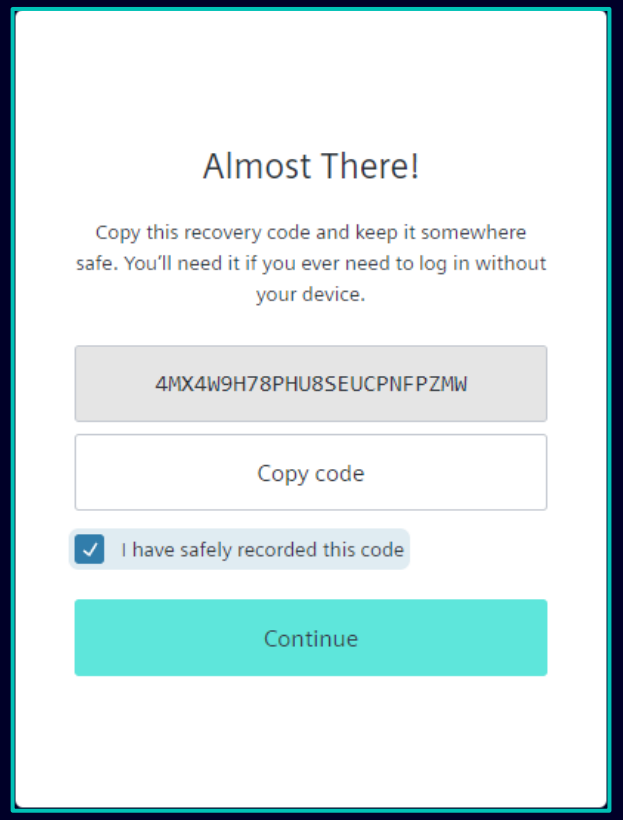
Google Authenticator oder ähnliches kann verwendet werden, wenn der Benutzer bereits den Google Authenticator oder eine ähnliche Authentifizierungs-App auf seinem Gerät installiert hat. Nach Nutzung dieser Option wird ein QR-Code gescannt, um den Einmalcode zu erstellen.

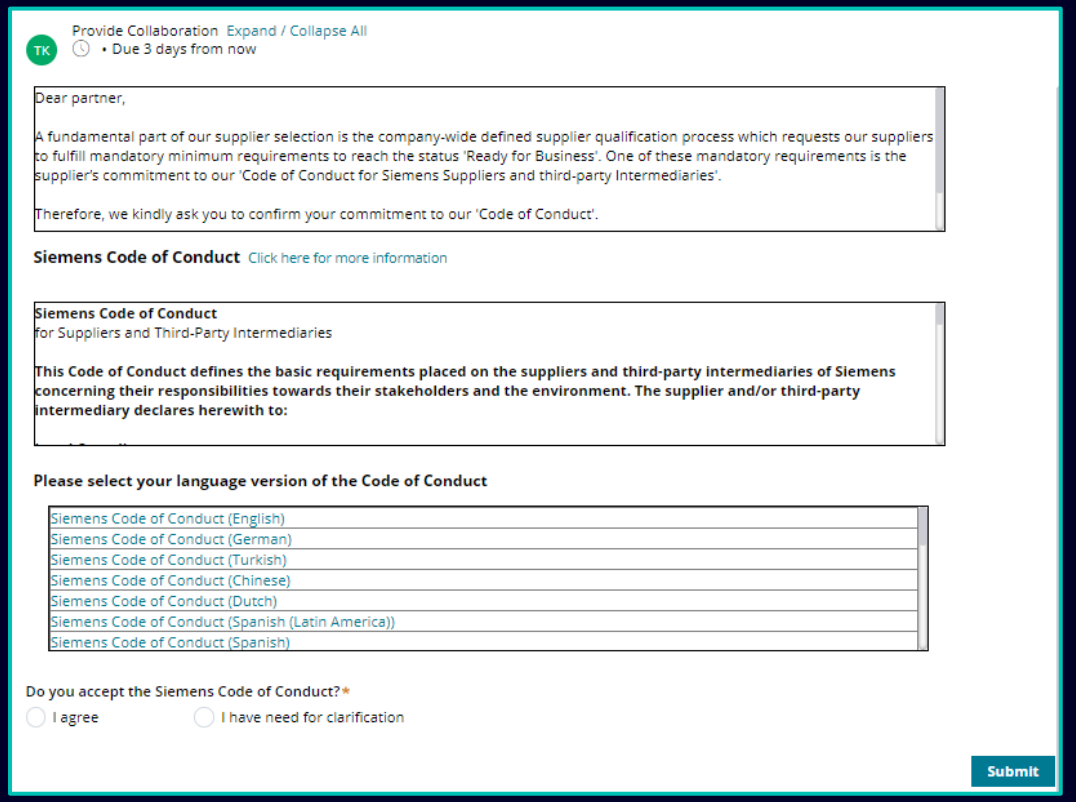
SIEMENS

Lieferantenstammdatenverwaltung (SMDM)
Inhalt

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten
Akzeptanz des Verhaltenskodex "Code of Conduct" (CoC)

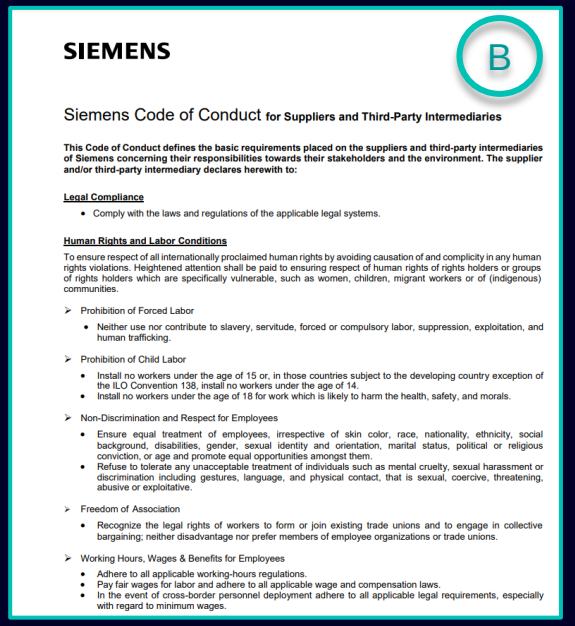


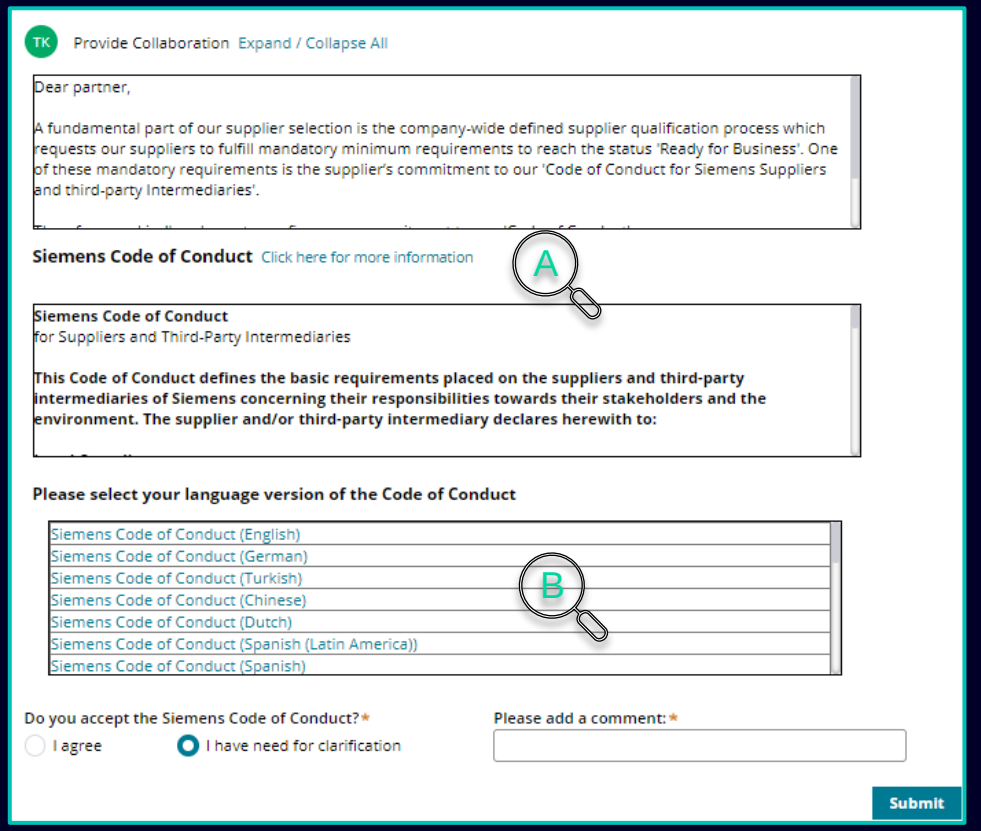


Nach erfolgreicher Authentifizierung werden Sie aufgefordert, den Siemens-Verhaltenskodex (CoC) zu akzeptieren (sofern dieser noch nicht in der SCM-Datenbank verfügbar ist). Weitere Informationen zur Akzeptanz des Verhaltenskodex finden Sie auf den nächsten Seiten.

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten
Akzeptanz des Verhaltenskodex "Code of Conduct" (CoC)

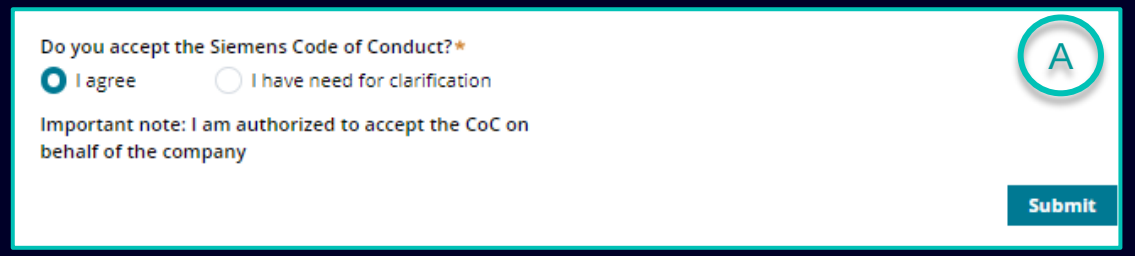


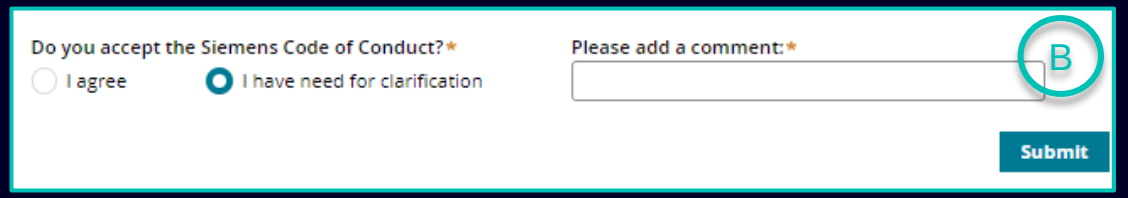


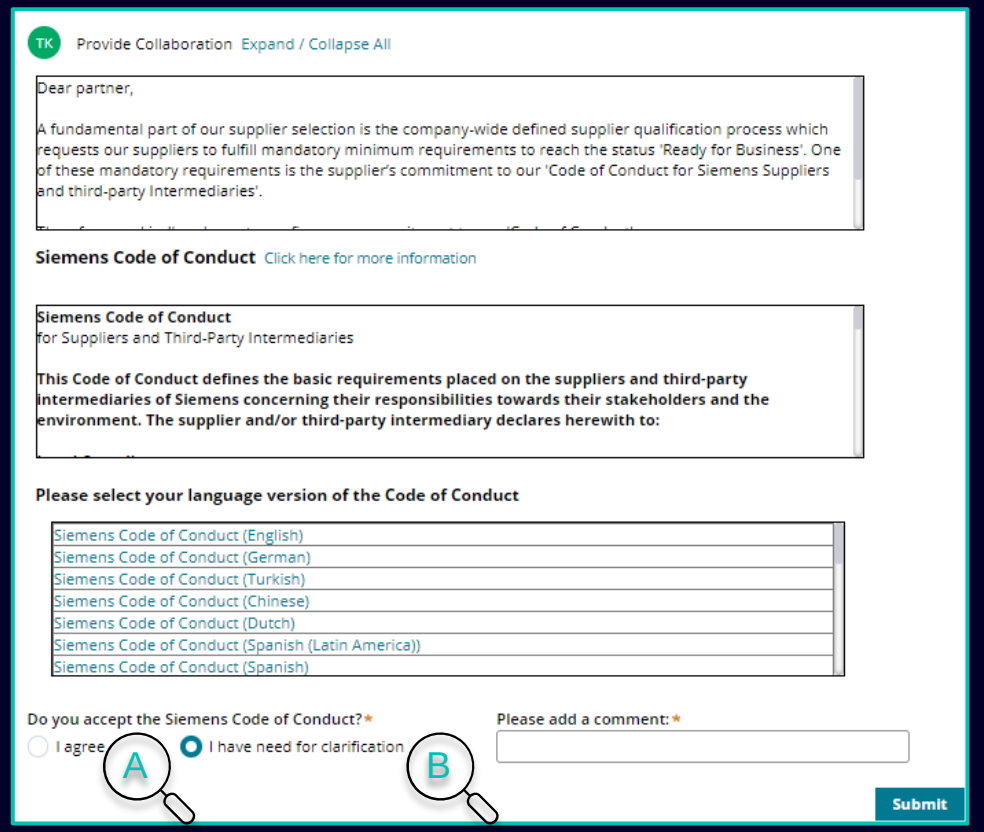
Nach erfolgreicher Authentifizierung werden Sie aufgefordert, den Siemens-Verhaltenskodex zu akzeptieren (sofern dieser noch nicht in der SCM-Datenbank verfügbar ist).
(A) Über den Link erhalten Sie weitere Detailinformationen zum Siemens-Verhaltenskodex (Code of Conduct).
(B) Der CoC steht in verschiedenen Sprachvarianten zur Verfügung..

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten
Akzeptanz des Verhaltenskodex "Code of Conduct" (CoC)





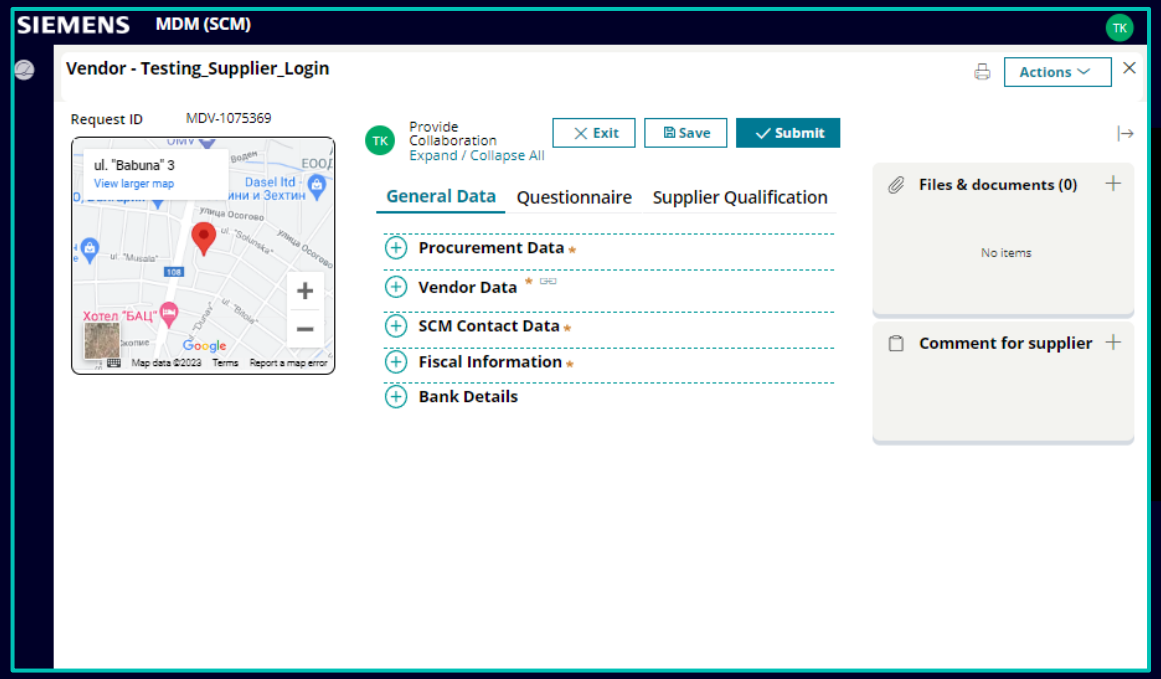


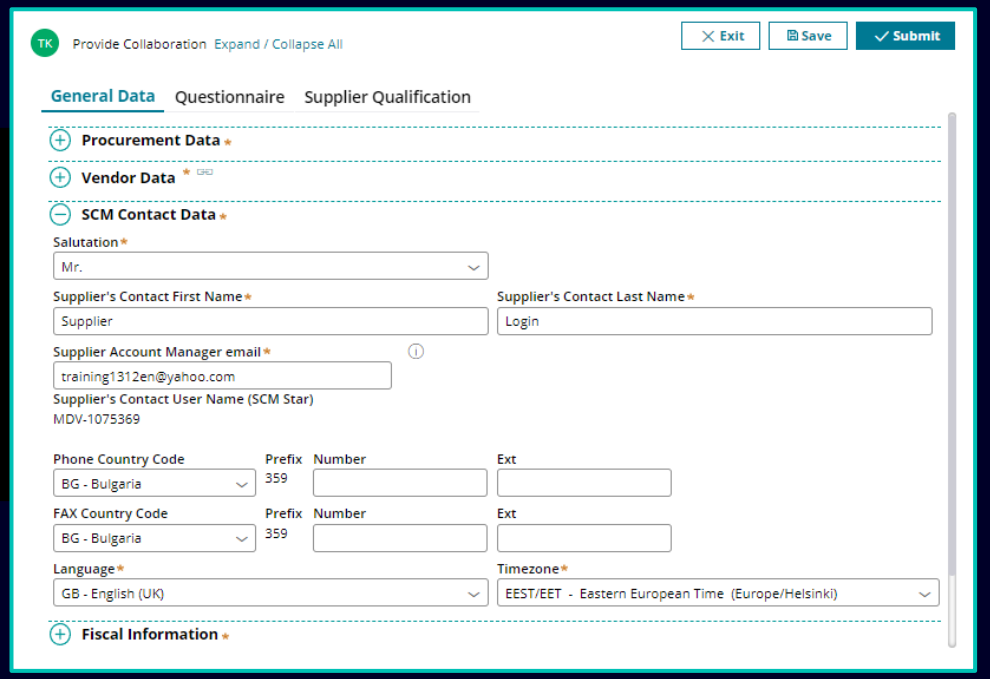
(A): Indem Sie dem Verhaltenskodex zustimmen, bestätigen Sie, dass Sie berechtigt sind, die Bedingungen des Verhaltenskodex im Namen ihres Unternehmens zu akzeptieren. Nach dem Absenden über "Submit" werden Sie zu Ihrer aktuellen Lieferantenstammdatenübersicht weitergeleitet.
(B): Im Falle von Rückfragen/ Klärungsbedarf tragen Sie bitte einen Kommentar mit Ihren Bedenken in das Textfeld ein und klicken auf "Submit“. Sie werden von Siemens kontaktiert.

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten

Daten, die überprüft/angepasst/hinzugefügt werden sollen – „Allgemeine Daten“



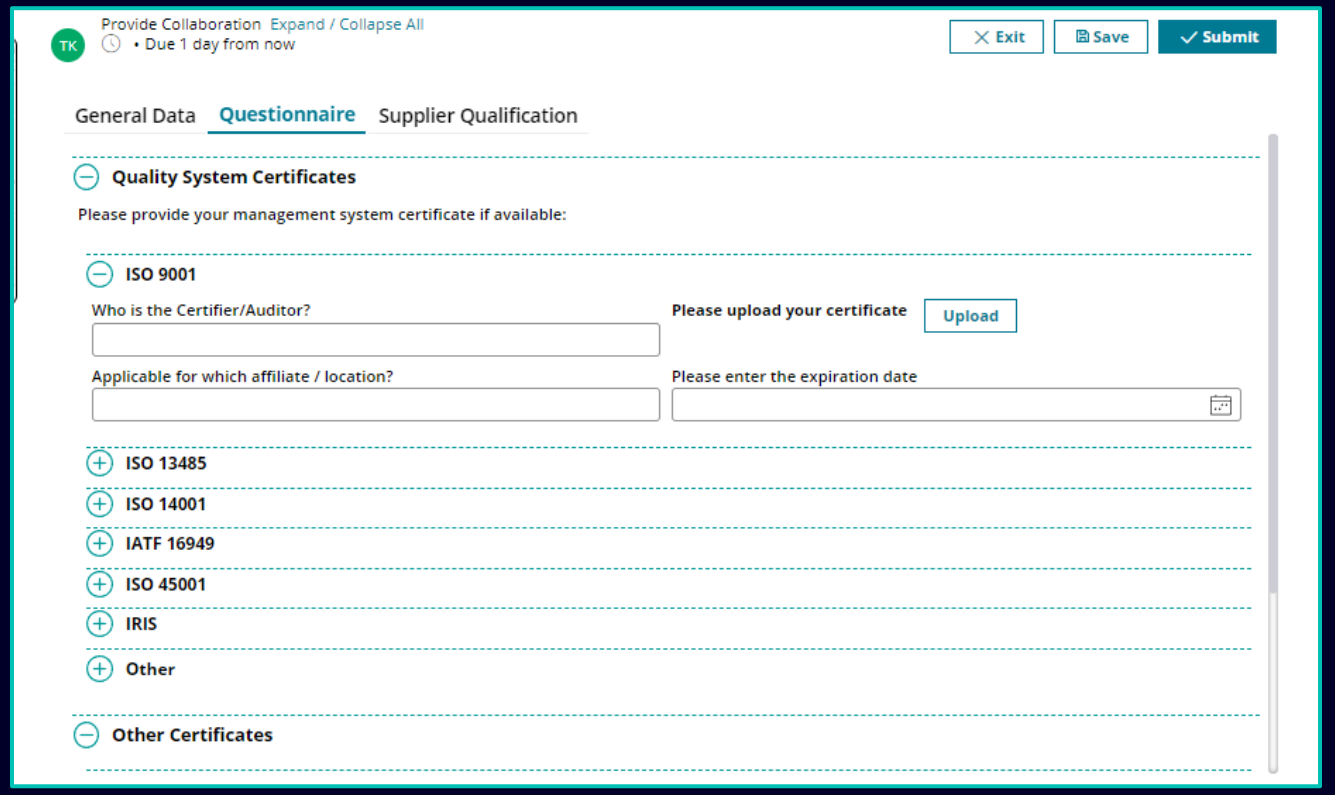


Nachdem Sie den Verhaltenskodex akzeptiert haben, können Sie die Lieferantenstammdaten im Abschnitt „Allgemeine Daten“ überprüfen. Öffnen Sie jeden Abschnitt, um den Inhalt zu überprüfen/ zu bearbeiten. Pflichtfelder sind mit einem Sternchen (*) gekennzeichnet.

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten

Zu überprüfende/ anzupassende/ ergänzende Daten – Spalte „Fragebogen“.

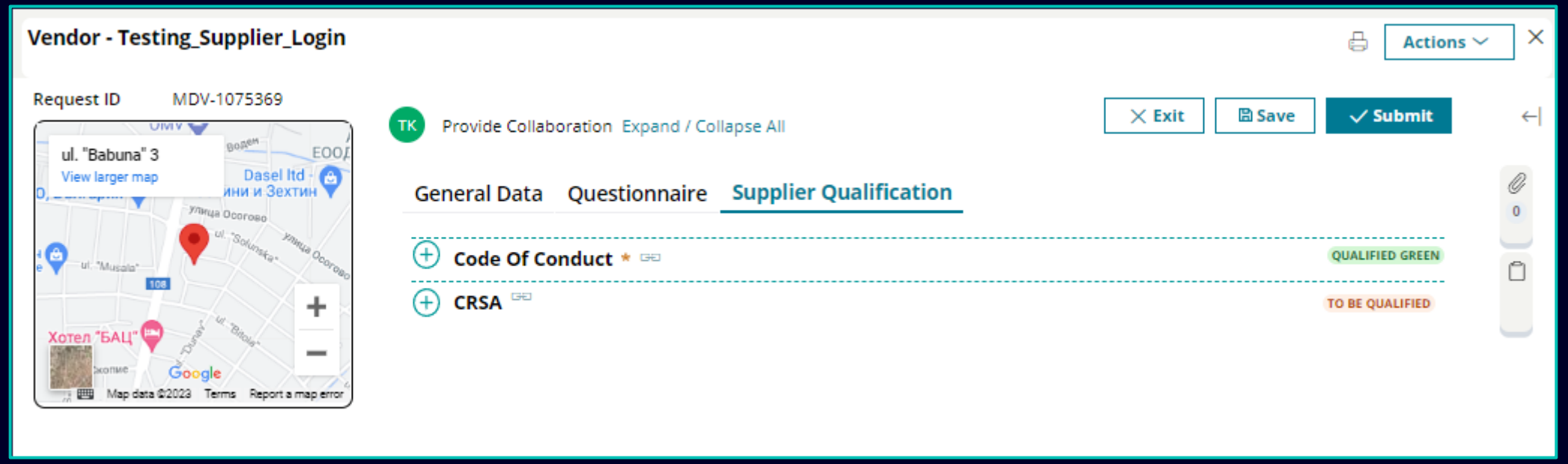


Unter der Registerkarte „Questionnaire (Fragebogen)“ können Sie gültige verfügbare Zertifikate hochladen. Falls das Hochladen eines Zertifikats verpflichtend ist, wird das entsprechende Feld mit einem Sternchen (*) markiert.

SIEMENS

Erfassung / Aktualisierung Ihrer Lieferantenstammdaten

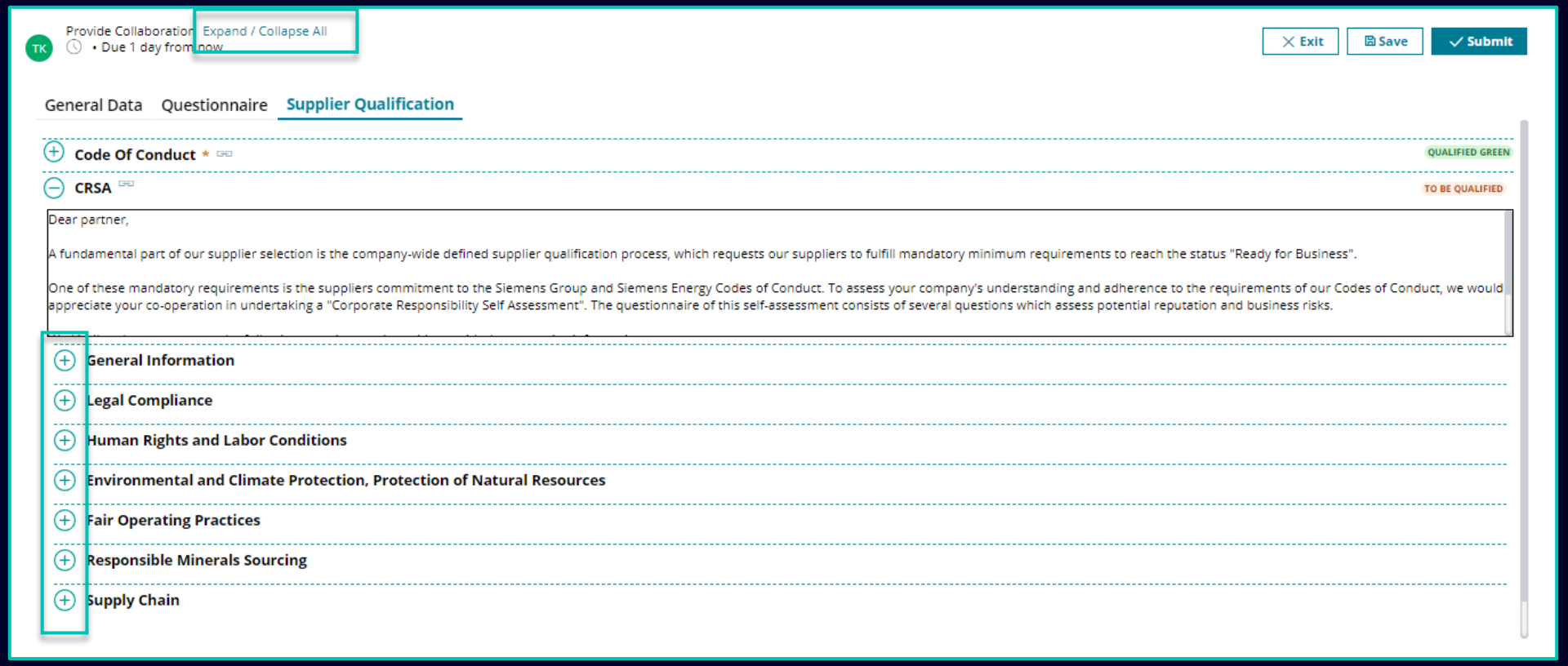
Zu überprüfende/ anzupassende/ ergänzende Daten – Spalte„Lieferantenqualifizierung“.



Auf der Registerkarte „Lieferantenqualifizierung“ finden Sie Angaben zu den erforderlichen Modulen zur Lieferantenqualifizierung. Sobald der Verhaltenskodex akzeptiert wurde, wird das Modul als „Qualified Green“ angezeigt (alle erforderlichen Informationen wurden bereitgestellt). Die Notwendigkeit der Erfüllung des Lieferantenqualifizierungsmoduls wird durch den farbigen Hinweis widergespiegelt. „To be Qualified“ bedeutet, dass die Erfüllung des Moduls erforderlich ist, um den Status „Ready for Business“ zu erreichen. Die letzte Option ist „Not relevant“ – das Qualifizierungsmodul ist nicht erforderlich.

SIEMENS

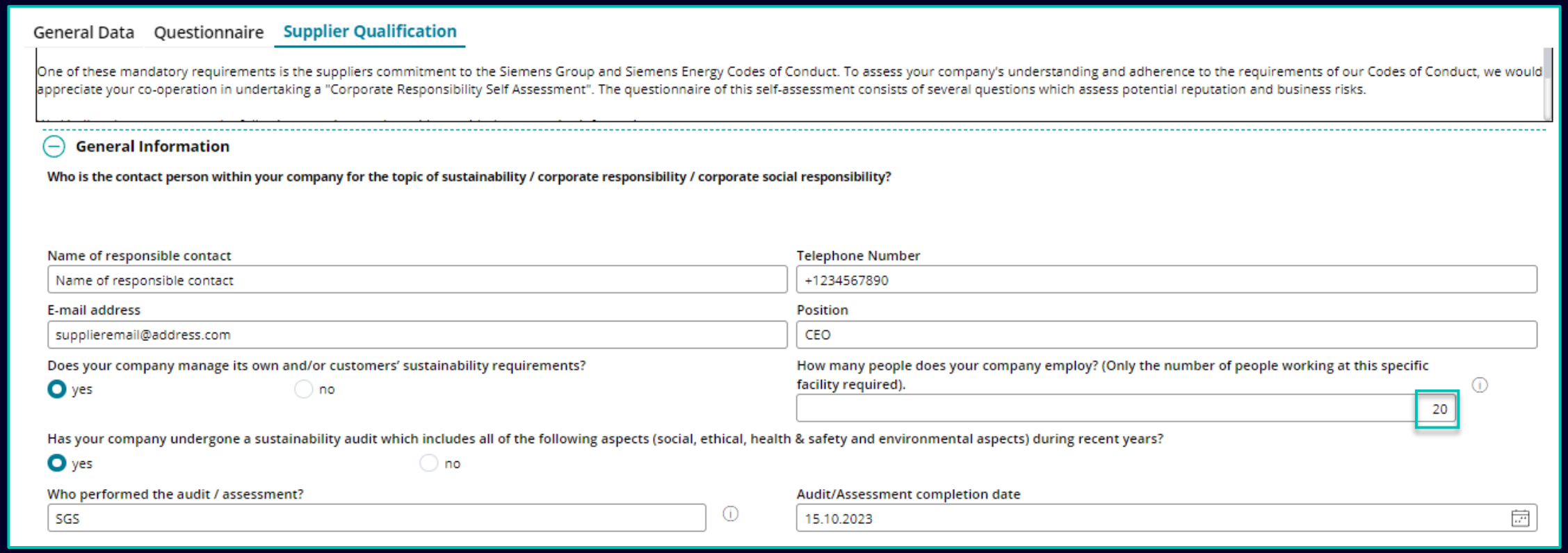
Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
1/6



Das CRSA-Qualifizierungsmodul (Corporate Responsibility Self-Assessment) besteht aus einem Lieferantenfragebogen, der in sieben spezifische Abschnitte unterteilt ist. Erweitern Sie das CRSA-Modul sowie jeden Abschnitt und füllen Sie alle Fragen aus (bei Unvollständigkeit werden die Fragen gelöscht). Sie können auch die Funktion „Expand/Collapse All“ verwenden.

SIEMENS

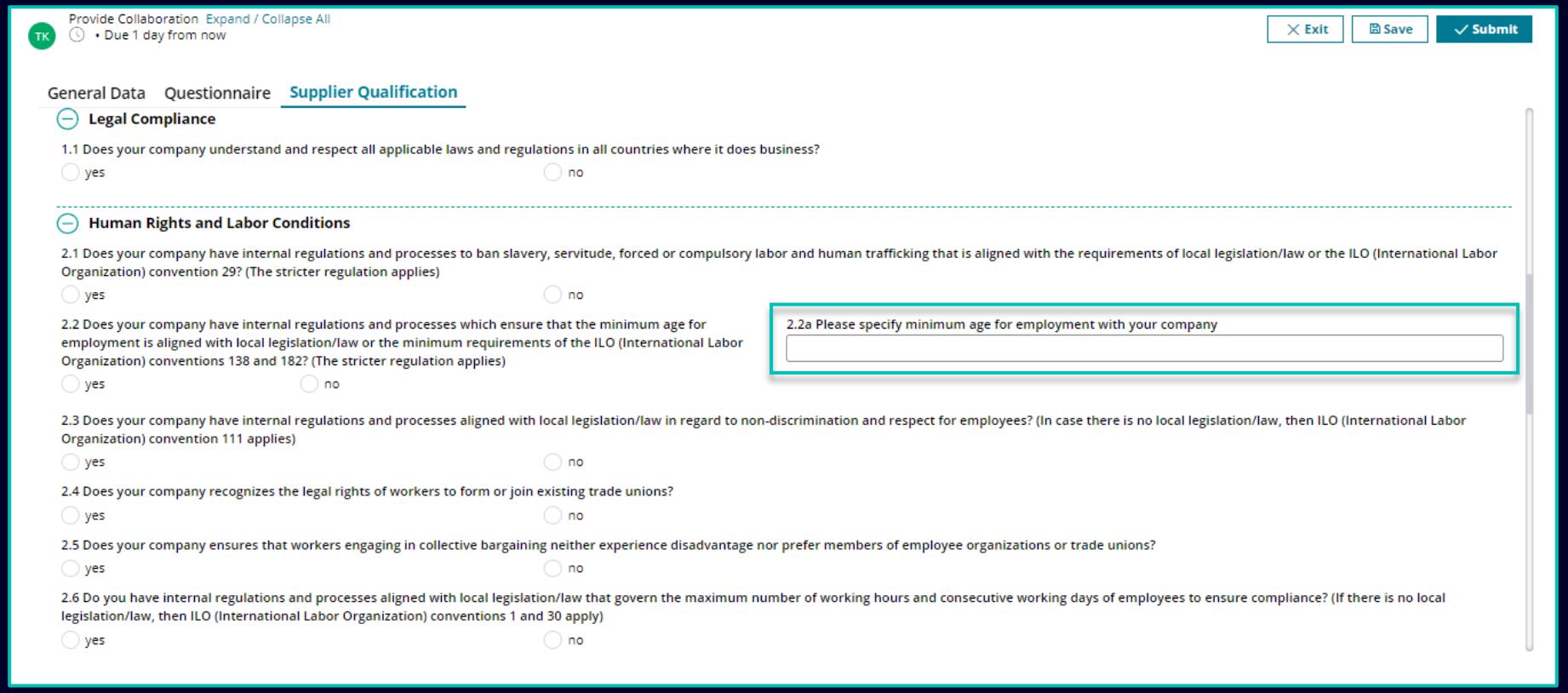
Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
2/6



Geben Sie im Abschnitt „General Information“ die Kontaktdaten und grundlegende Informationen zum Lieferantenunternehmen ein. Klicken Sie auf das Info-Symbol neben jeder Frage, um weitere Informationen zum Fachgebiet zu erhalten, z. B. „Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?“ – Wenn Sie als Einpersonen-Unternehmen gelten und keine Mitarbeiter haben, dann tragen Sie 0 ein. Der CRSA-Fragebogen ist für Sie nicht anwendbar. Sobald 0 ausgefüllt ist, werden alle anderen CRSA-Abschnitte deaktiviert.

SIEMENS

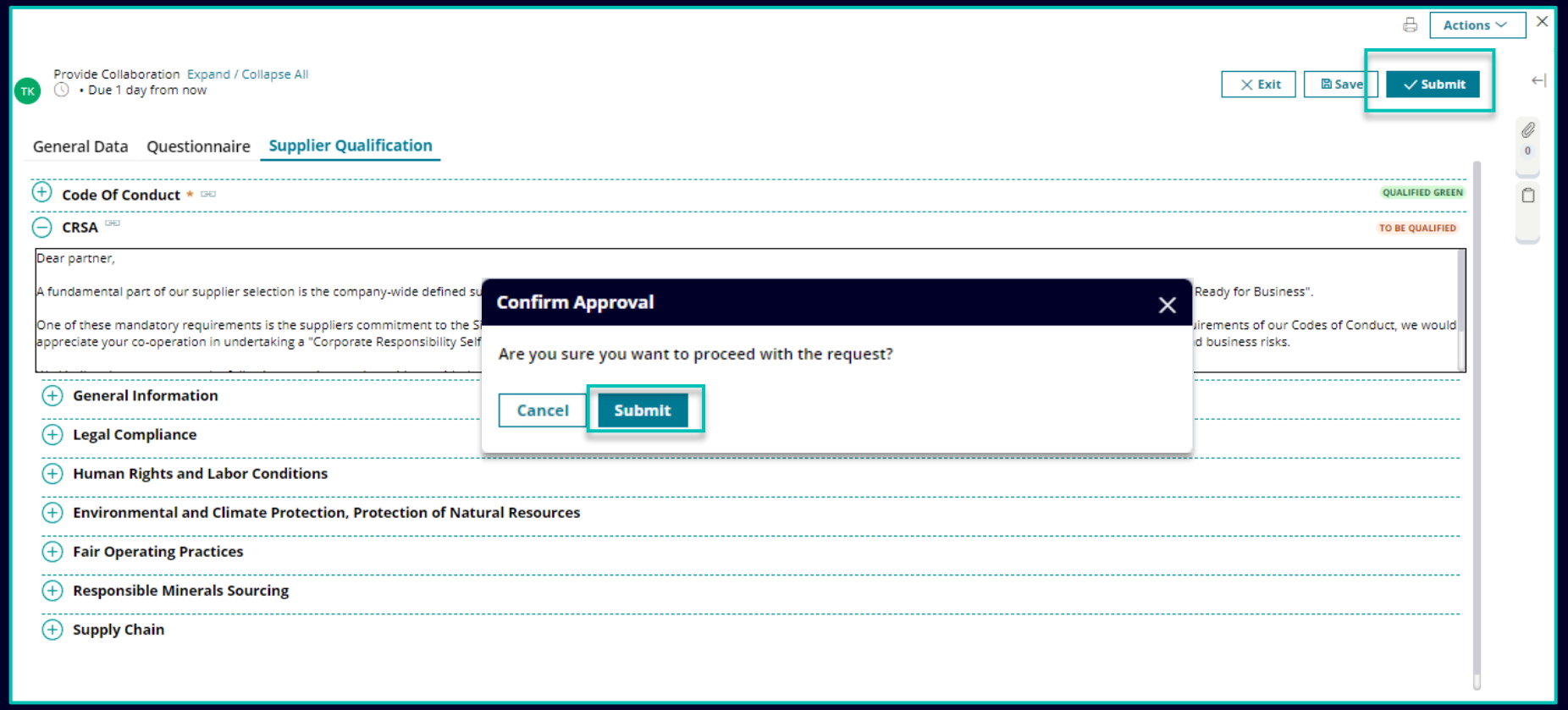
Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
3/6



Öffnen Sie jeden einzelnen Abschnitt und beantworten Sie jede Frage ein.
Vergessen Sie nicht, Frage 2.2a (Mindestalter für die Beschäftig in Ihrem Unternehmen) auszufüllen.

SIEMENS

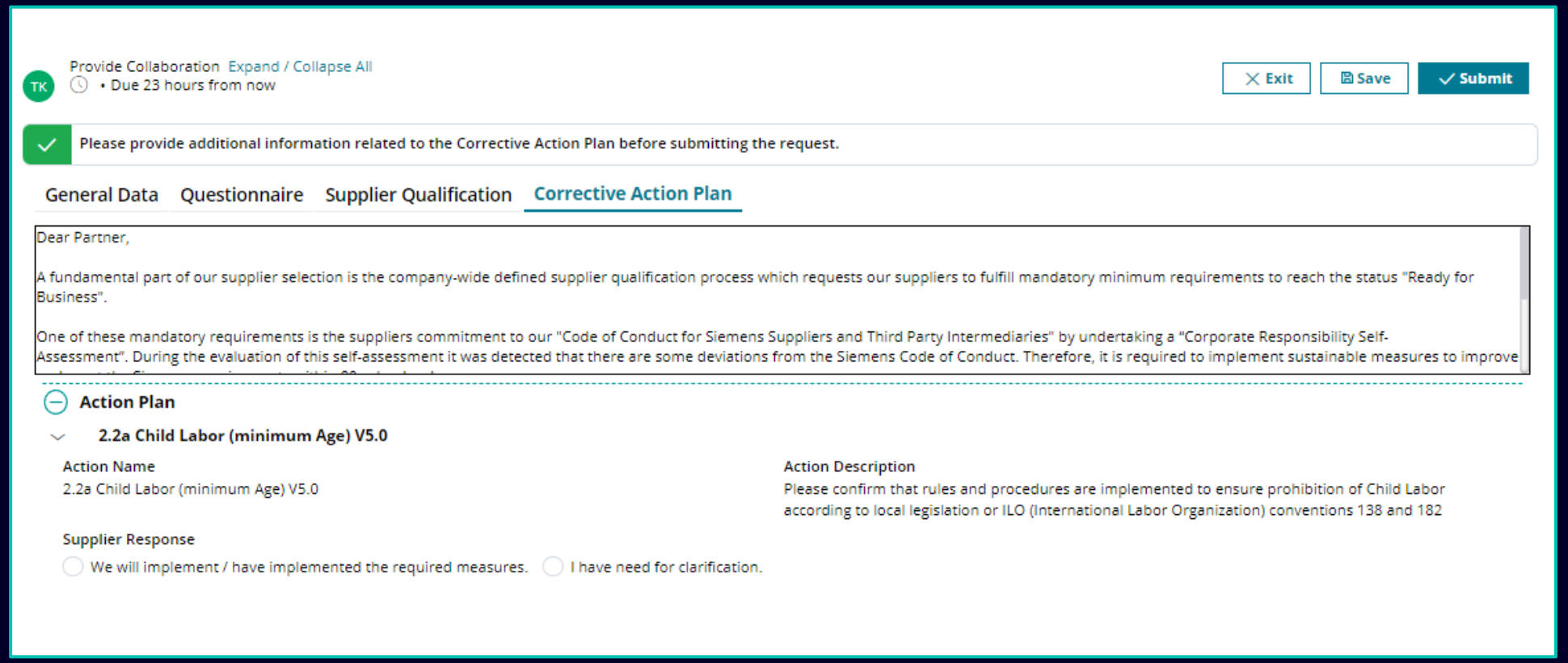
Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
4/6



Nachdem alle Fragen in jedem Abschnitt ausgefüllt sind, klicken Sie auf „Submit“ und bestätigen Sie das Absenden.

SIEMENS

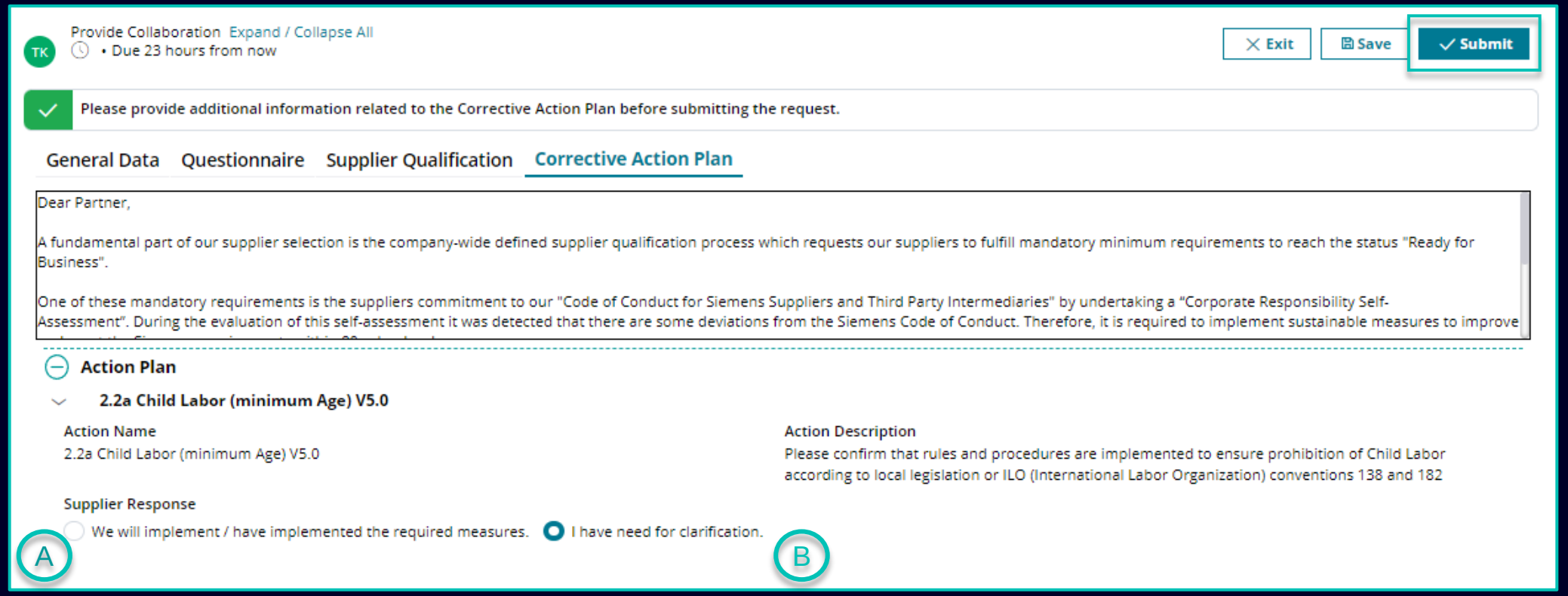
Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
5/6



Nach dem Absenden der Lieferantenqualifizierungsanfrage überprüft das System die bereitgestellten Antworten. Falls Korrekturmaßnahmen auf der Grundlage gegebener Antworten erforderlich sind, erscheint eine neue Registerkarte „Corrective Action Plan“ – die ursprünglichen Antworten bleiben schreibgeschützt. Erweitern Sie den Abschnitt „Action Plan“, um die Aktionspunkte zu überprüfen.

SIEMENS

Akzeptanz des Corporate Responsibility Self-Assessment (CRSA)
6/6



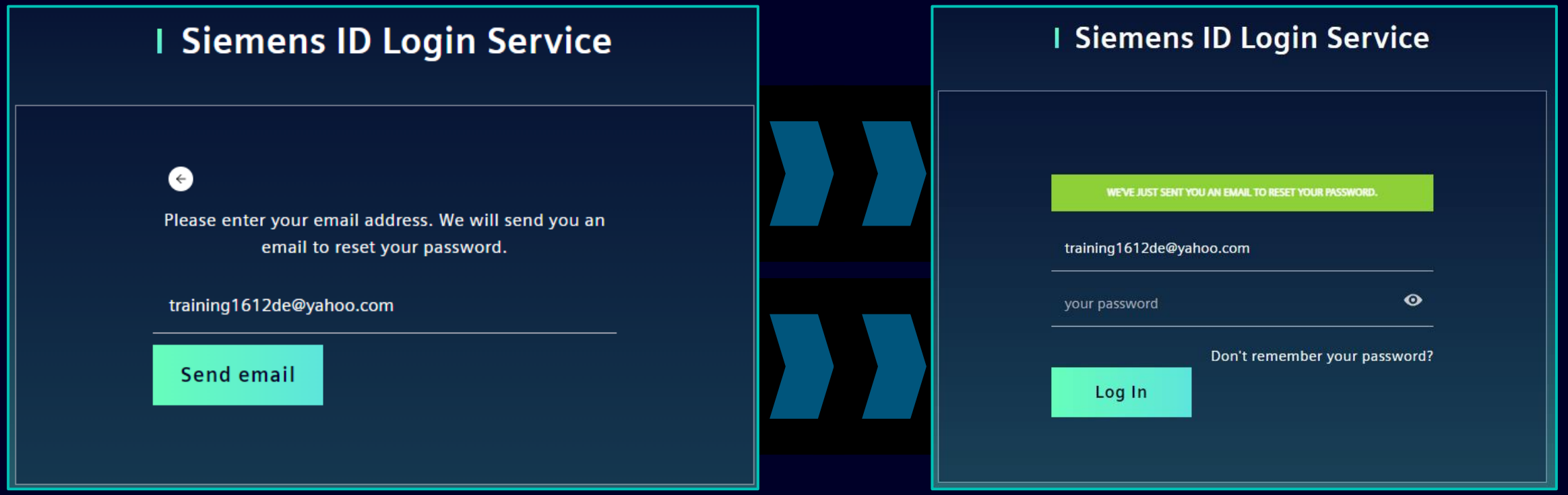
Geben Sie zu jedem Aktionspunkt die entsprechende Antwort: (A) Markieren Sie die Frage entsprechend, wenn die erforderlichen Maßnahmen umgesetzt werden oder bereits umgesetzt wurden. (B) Falls weitere Erläuterungen erforderlich sind, markieren Sie die Frage entsprechend. Für jede mit (B) markierte Frage werden Sie vom GBS-Team zur weiteren Klärung kontaktiert.
Nachdem Sie alle Antworten eingegeben haben, klicken Sie auf „Submit“, um die Qualifizierungsanforderung abzuschließen.

SIEMENS

Lieferantenstammdatenverwaltung (SMDM)
Inhalt

SIEMENS

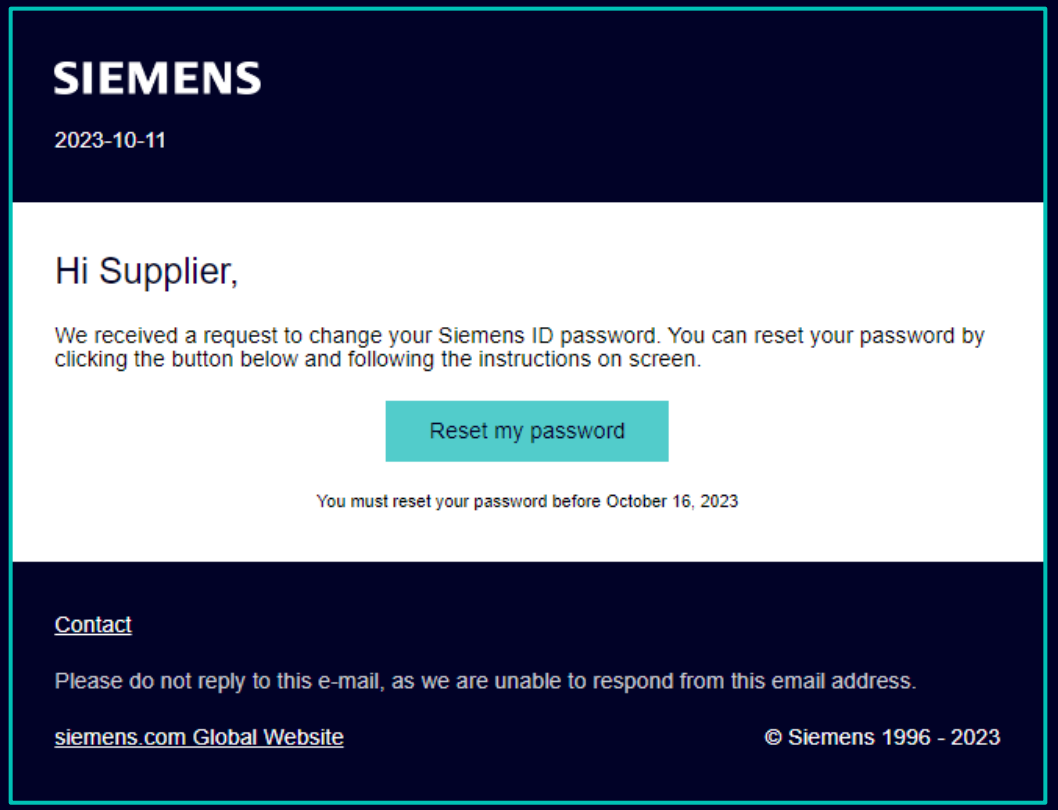
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen



Geben Sie Ihre E-Mail-Adresse ein (dieselbe E-Mail-Adresse wie auf der Seite 6 angezeigt) und klicken Sie auf „Send Email“. Sie erhalten eine E-Mail, um Ihr Passwort erneut zurückzusetzen.

SIEMENS

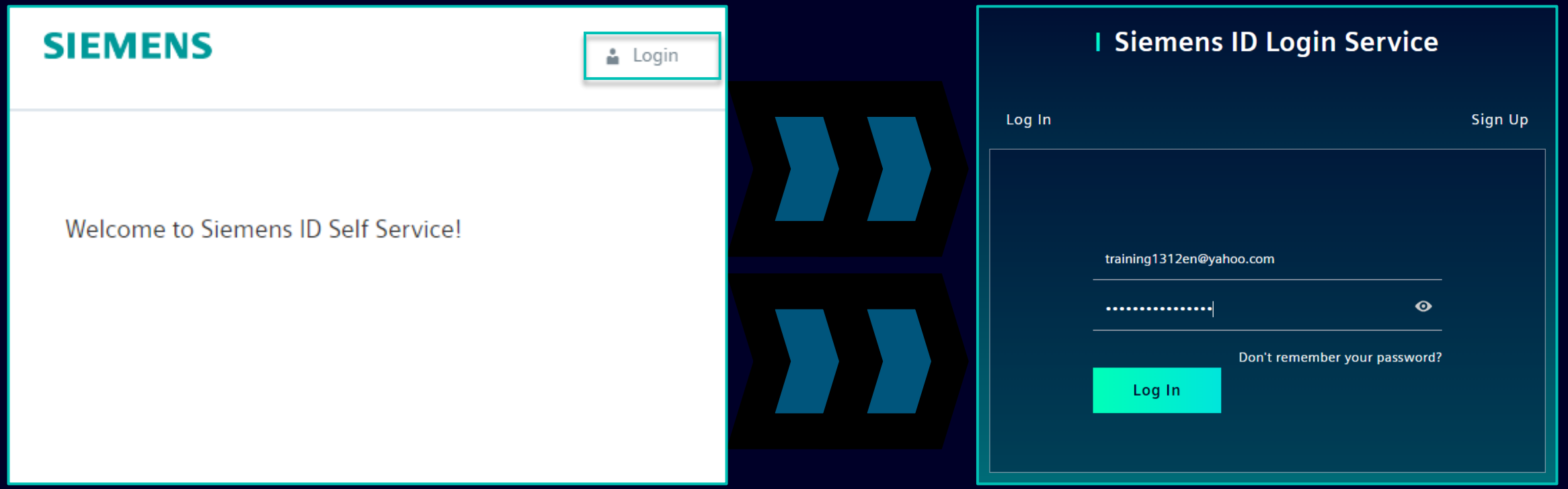
Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen



Öffnen Sie die E-Mail und klicken Sie auf „Reset my password“. Sie werden zur ersten Siemens-Anmeldeseite weitergeleitet, wo Sie Ihr neu festgelegtes Passwort zurücksetzen können. Dann fahren Sie hier fort.

SIEMENS

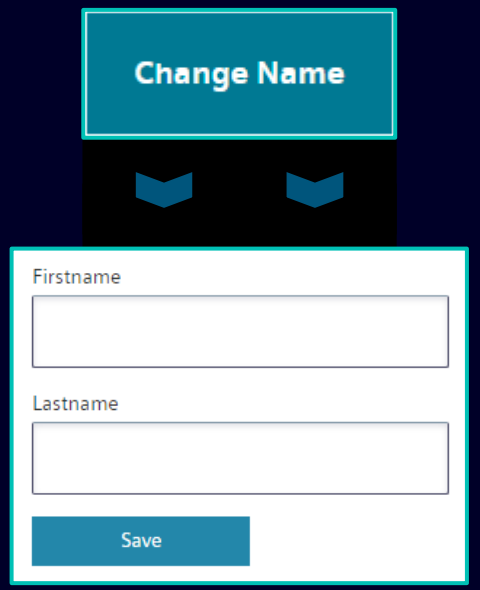
So setzen Sie die Authentifizierungsmethode zurück



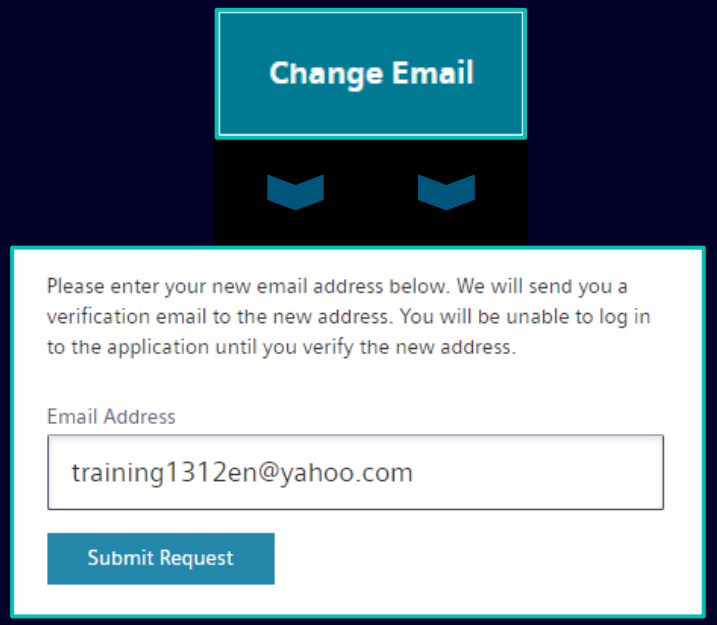
Bitte gehen Sie auf https://uss.login.siemens.com und klicken auf „Login“; Geben Sie auf der nächsten Seite Ihre E-Mail-Adresse und Ihr Passwort ein und klicken Sie auf „Login“.

SIEMENS

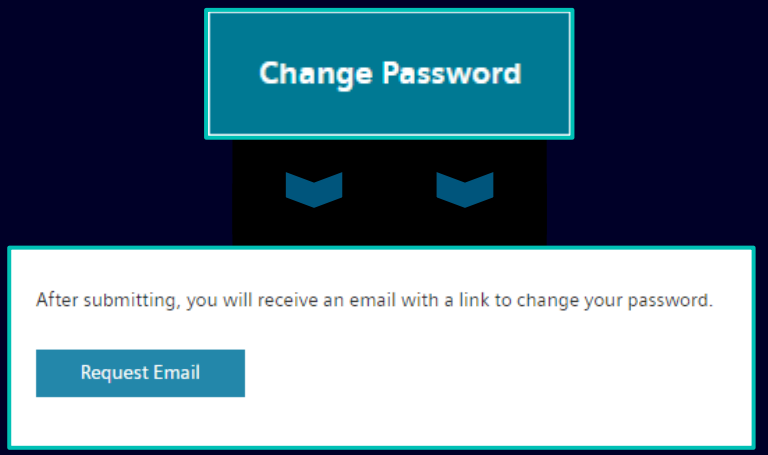
So setzen Sie die Authentifizierungsmethode zurück
Änderung der Kontoinformationen



Das Ändern Ihres Vor- und Nachnamens hat keinen Einfluss auf die Authentifizierungslogik.



Wenn Sie Ihre E-Mail-Adresse ändern, wird der Anwendungszugriff deaktiviert, bis die neue E-Mail-Adresse bestätigt wird. Anschließend kann die neue E-Mail-Adresse für die bestehende Authentifizierungsmethode verwendet werden.

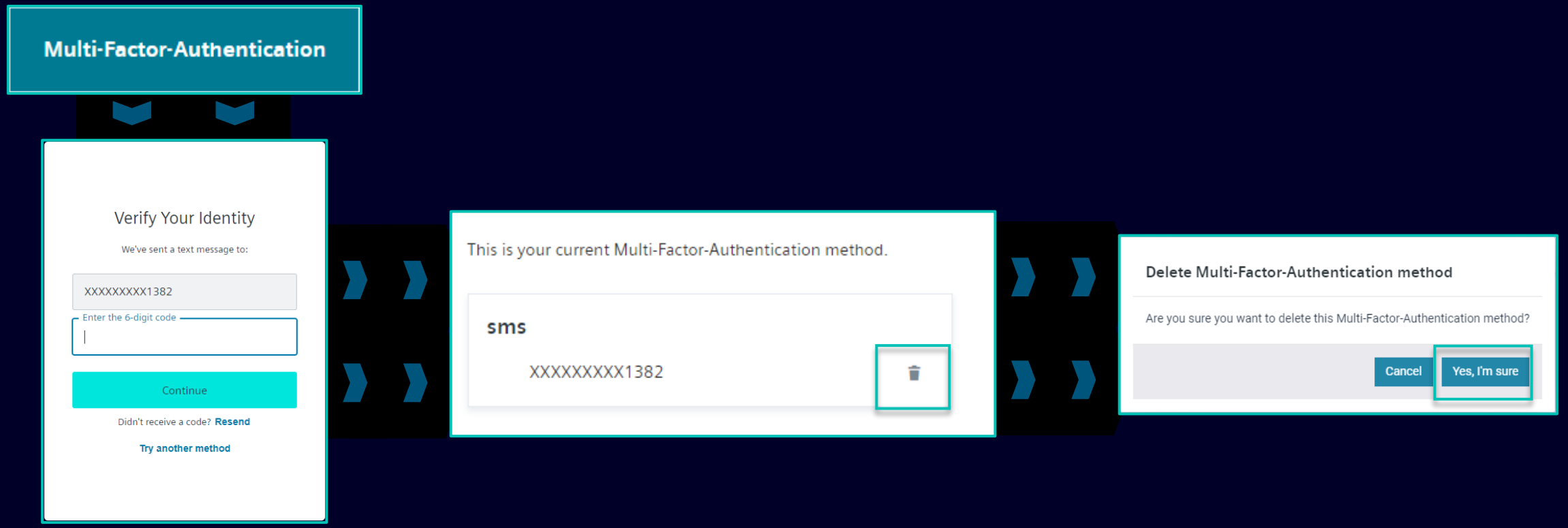


Das Zurücksetzen Ihres Passworts hat keine Auswirkungen auf die zweite Authentifizierungsmethode. Nach dem Zurücksetzen des Passworts wird das aktuelle zweite Authentifizierungssetup voreingestellt.

Nach Angabe der zweiten Authentifizierungsmethode werden Sie zu den oben genannten Profileinstellungen weitergeleitet.

SIEMENS

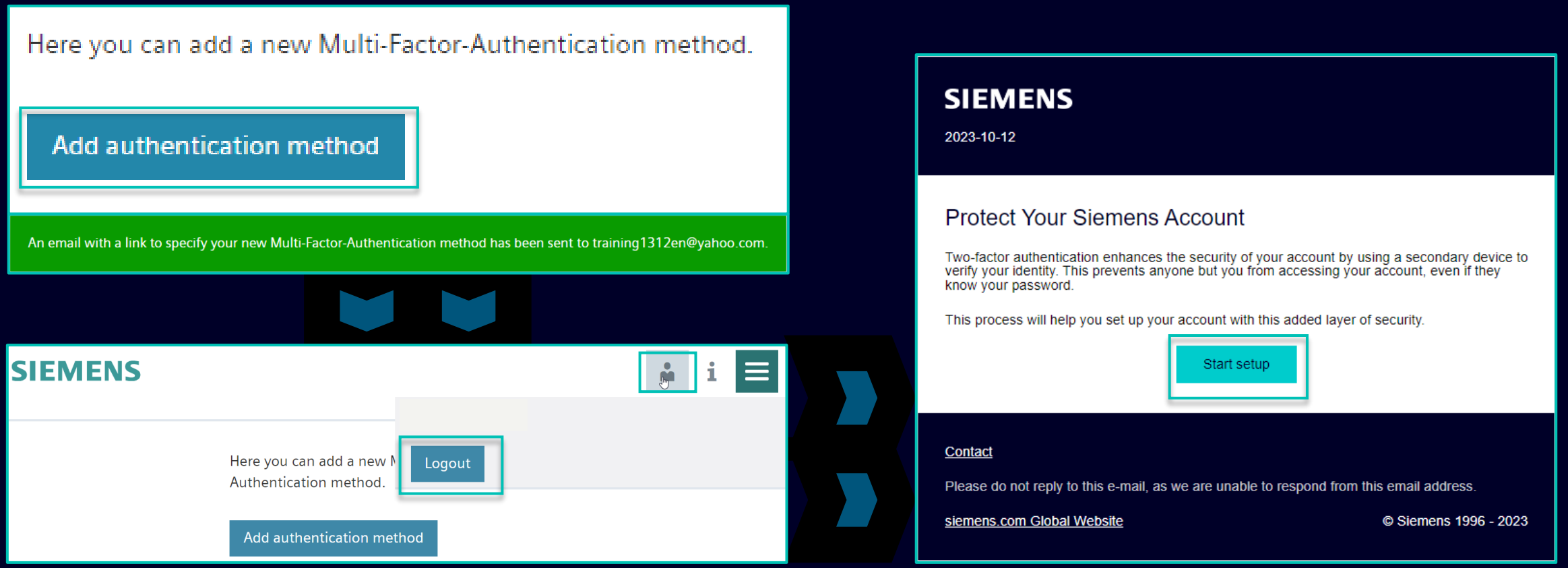
So setzen Sie die Authentifizierungsmethode zurück
Änderung der Multi-Faktor-Authentifizierungsmethode



Um Ihre Multi-Faktor-Authentifizierungsmethode zurückzusetzen, klicken Sie auf „Multi-Factor-Authentication“ – Sie werden weitergeleitet, um die aktuell eingestellte Authentifizierungsmethode anzugeben. Wählen Sie nach der Anmeldung das Löschsymbol aus und bestätigen Sie das Zurücksetzen. Falls Sie versuchen, die zweite Authentifizierungsmethode zurückzusetzen, weil die zweite Authentifizierungsmethode für Sie nicht verfügbar ist (z. B. Telefon verloren, Zugriff auf die Guardian-App oder andere zweite Authentifizierungs-Apps verloren), klicken Sie hier für die Anleitung.

SIEMENS

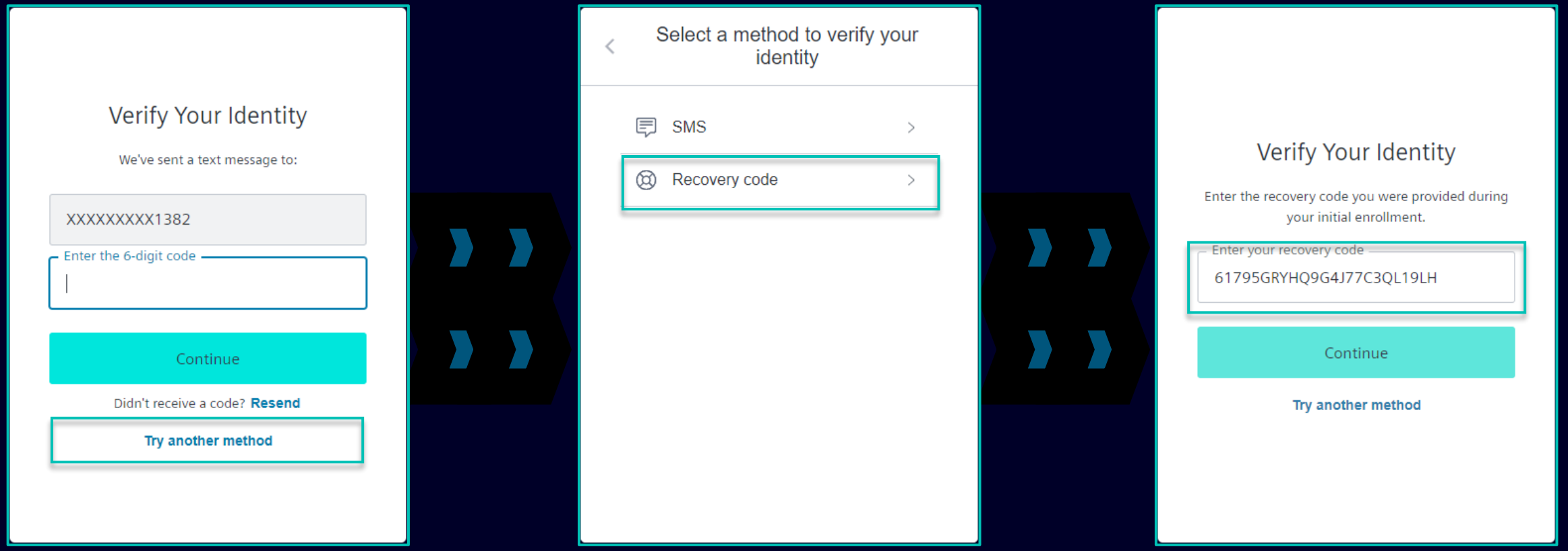
So setzen Sie die Authentifizierungsmethode zurück
Änderung der Multi-Faktor-Authentifizierungsmethode



Nachdem Sie die aktuelle Authentifizierungsmethode gelöscht haben, müssen Sie eine neue Multi-Faktor-Authentifizierungsmethode festlegen. Klicken Sie auf „Add authentication method“ und Sie erhalten eine E-Mail. **Es ist wichtig, dass Sie sich von Ihrem Konto abmelden, bevor Sie mit der Einrichtung einer neuen zweiten Authentifizierungsmethode fortfahren.** Gehen Sie dann zu Ihrem E-Mail-Posteingang, klicken Sie auf „Start setup“ und fahren Sie wie hier fort.

SIEMENS

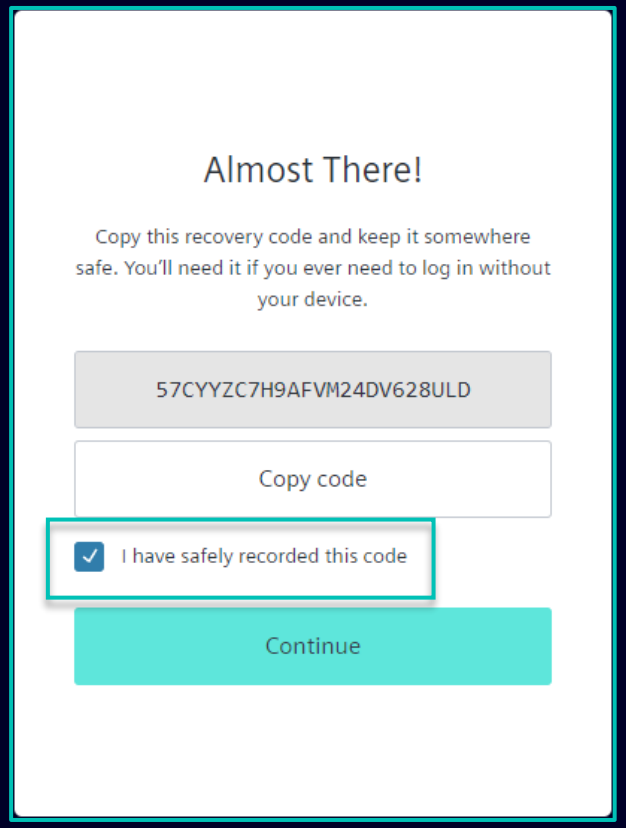
So setzen Sie die Authentifizierungsmethode zurück
Anmeldung über Wiederherstellungscode



Wenn Sie die zweite Authentifizierungsmethode ändern müssen oder die zweite Authentifizierung derzeit nicht bereitstellen können, können Sie sich mit dem Wiederherstellungscode anmelden, den Sie bei Ihrer ersten Anmeldung erhalten haben. In diesem Fall, wenn Sie nach der zweiten Authentifizierung gefragt werden, wählen Sie „Andere Methode ausprobieren“ und wählen Sie die Option „Recovery code“. Kopieren Sie Ihren Wiederherstellungscode und klicken auf „Continue“.

SIEMENS

So setzen Sie die Authentifizierungsmethode zurück
Anmeldung über Wiederherstellungscode



Sie erhalten einen neuen Wiederherstellungscode. Bitte stellen Sie sicher, dass Sie den neuen Wiederherstellungscode durch den Alten ersetzen. Der alte Wiederherstellungscode wird deaktiviert, nachdem Sie einen neuen Code erhalten haben. Nachdem Sie Ihren neuen Wiederherstellungscode gespeichert haben, klicken Sie auf „Continue“.

SIEMENS

Lieferantenstammdatenverwaltung (SMDM)
Inhalt

SIEMENS

Further communication material and wrap-up
Multimedia touch points

1 Supplier Portal

- Informationen zu SCM STAR im Allgemeinen
- Neuigkeiten und Informationen, um Sie auf dem Laufenden zu halten
- Zugriff auf Schulungsmaterial (Download Center)

2 First level support

User Help Desk

The User Help Desk is available from Monday to Friday, 07.00 a.m. – 08.00 p.m. CET. Supported Languages: English and German.

GBS Portal: **Open a ticket here**

Phone Support is no longer available since 01.10.2023

- Eröffnen Sie ein Ticket per E-Mail – klicken Sie hier

SIEMENS

Vielen Dank

SIEMENS