Konferenz- und Gast-Netz tubs-guest

Das Gauß-IT-Zentrum bietet den Instituten und Einrichtungen mit dem Dienst 1109 „Konferenz- und Gast-Netz für Institute und Einrichtungen“ die Möglichkeit, für deren Gäste einen Zugang zum Internet zur Verfügung zu stellen. Bestandteil des Dienstes ist eine Selbstbedienungsschnittstelle für DV-Koordinatoren zur Einrichtung und Verwaltung von zeitlich befristeten und personenbezogenen Gast-Benutzerkennungen. Sie erhalten mit diesem Dienst eine komfortable und zeitgemäße Nutzungsmöglichkeit, um Ihren Gästen Internetzugang über WLAN so anbieten zu können, wie es auch in anderen Bereichen (Hotels, HotSpots) üblich ist. Das Gauß-IT-Zentrum stellt Ihnen über die Selbstbedienungsschnittstelle die nötigen Mittel zur Verfügung, den einschlägigen Vorgaben gerecht werden zu können. Dieses Dokument beschreibt die Nutzung der Selbstbedienungsschnittstelle.

> Als **Gast** oder **Konferenzteilnehmer** wenden Sie sich bitte an Ihre **Ansprechpartner** in Ihrem gastgebenden **Institut**.

DV-Koordinatoren beantragen WLAN Gast-Kennungen über folgendes Sponsoren-Portal:

- https://tubs-guest.tu-braunschweig.de

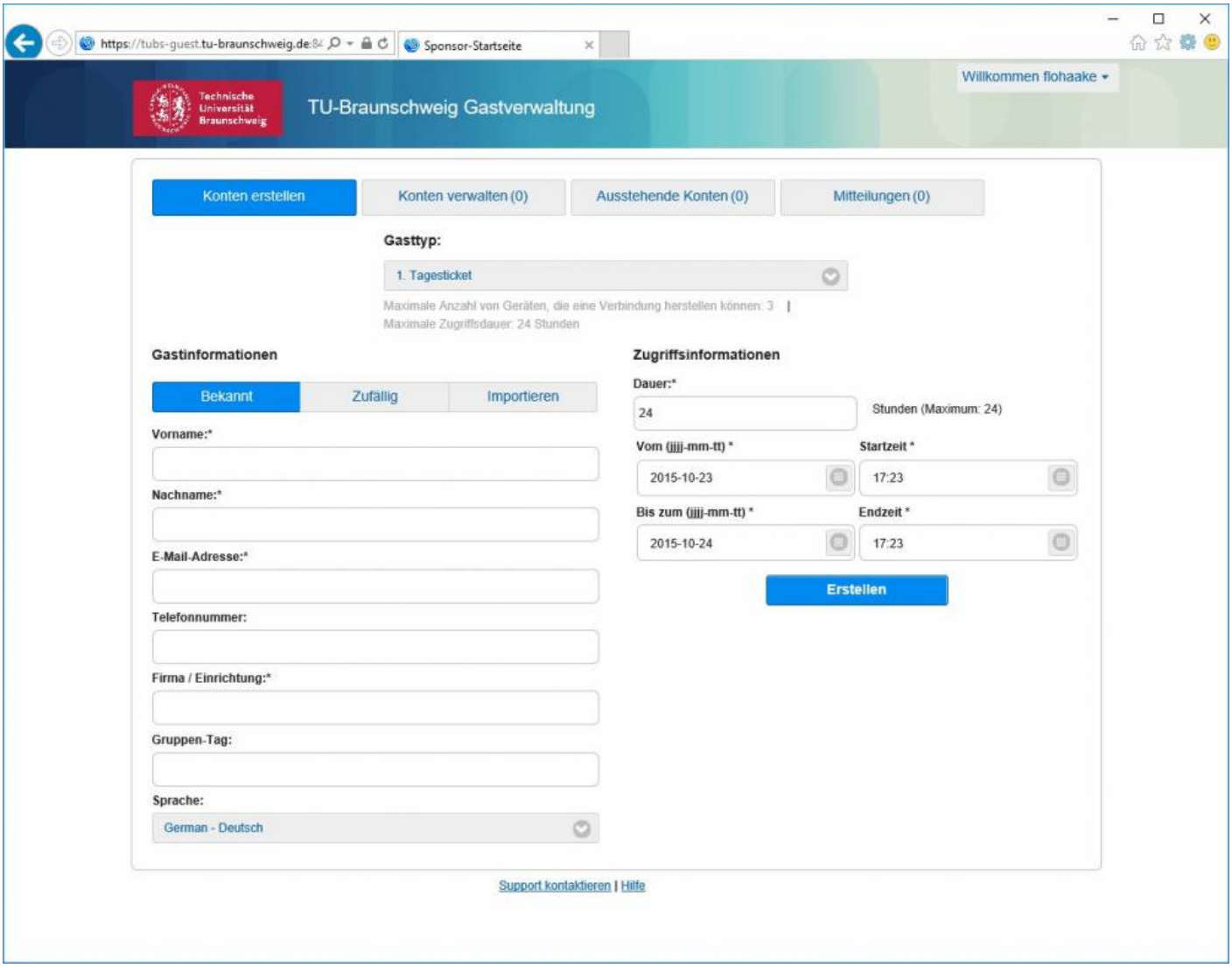
Darüber hinaus weisen wir darauf hin, dass bei Veranstaltungen mit mehr als 100 Teilnehmern eine Mitteilung über das Ihnen bekannte Kontaktformular zwingend benötigt wird. Das Formular erreichen Sie unter unserem Kontakt-Formular. Wir benötigen diese Information, damit u.a. ausreichend IP-Adressen zur Verfügung stehen.

> **Die maximale Verbindungsgeschwindigkeit für Mitarbeiter und Studierende der TU Braunschweig, die sich mit ihrer TUBS-ID im Gast-WLAN anmelden, wird begrenzt.**

> **Es wird empfohlen die Verbindung zum eduroam einzurichten.**

Nutzung durch DV-Koordinatoren

Die Selbstbedienungsschnittstelle zum Erstellen von Gast-Kennungen erreichen Sie unter der URL http://tubs-guest.tu-braunschweig.de aus dem Netz der TU Braunschweig (ggf. bitte per VPN einloggen). Hier loggen Sie sich mit Ihrer TUBS-ID ein. Nur bei uns im Gauß-IT-Zentrum eingetragene DV-Koordinatoren können diese Schnittstelle benutzen. Nach erfolgreichem Login wird die Übersichtsseite der Selbstbedienungsschnittstelle angezeigt.



Erstellen von Gast-Kennungen für tubs-guest

Ihnen als DV-Koordinator stehen zwei Optionen für die Erstellung von Gast-Kennungen zur Verfügung:

- Personalisierte Gast-Kennung erstellen (Reiter „Bekannt“)

- Mehrere Gast-Kennungen erstellen (Reiter „Zufällig“)
- Mehrere Gast-Kennungen via CSV-Datei importieren (Reiter „Importieren“)

Zeitprofile

Beim Anlegen von Gast-Benutzerkennungen kann bei jeder der vorgenannten Möglichkeiten ein Zeitprofil ausgewählt werden. Es stehen drei Zeitprofile zur Auswahl:

- Tagesticket
- Wochenticket
- Monatsticket
- Quartalsticket

Wenn Sie das Zeitprofil „Tagesticket“ auswählen, werden Gast-Kennungen mit einem Gültigkeitszeitraum von 24 Stunden ab dem ersten Login generiert. Dieses Zeitprofil empfehlen wir für Tagesgäste. Analog hierzu gelten Wochen-, Monats- bzw. Quartalstickets maximal sieben, 31 bzw. 180 Tage. Wir behalten uns vor abgelaufene Gast-Benutzerkennungen **nach 31 Tagen** zu löschen.

Der Gültigkeitszeitraum darf maximal 180 Tage umfassen. Das Erstellen von Gast-Kennungen mit diesem Zeitprofil soll nicht **mehr als drei Monate** im Voraus erfolgen.

In der Regel werden die personalisierten Zugangsdaten mit Benutzeranleitung durch Sie als DV-Koordinator ausgedruckt und Ihren Gästen ausgehändigt. Sofern eine E-Mail-Adresse hinterlegt wurde, besteht darüber hinaus die Möglichkeit, die Zugangsdaten mit Benutzeranleitung direkt über das System dem Gast zuzusenden. Bei Angabe einer Mobilfunknummer haben Sie weiterhin die Möglichkeit dem Gast eine SMS mit den Zugangsdaten zu schicken. Bitte beachten Sie auch die Ausführungen im Abschnitt „Aufzeichnungspflichten“.

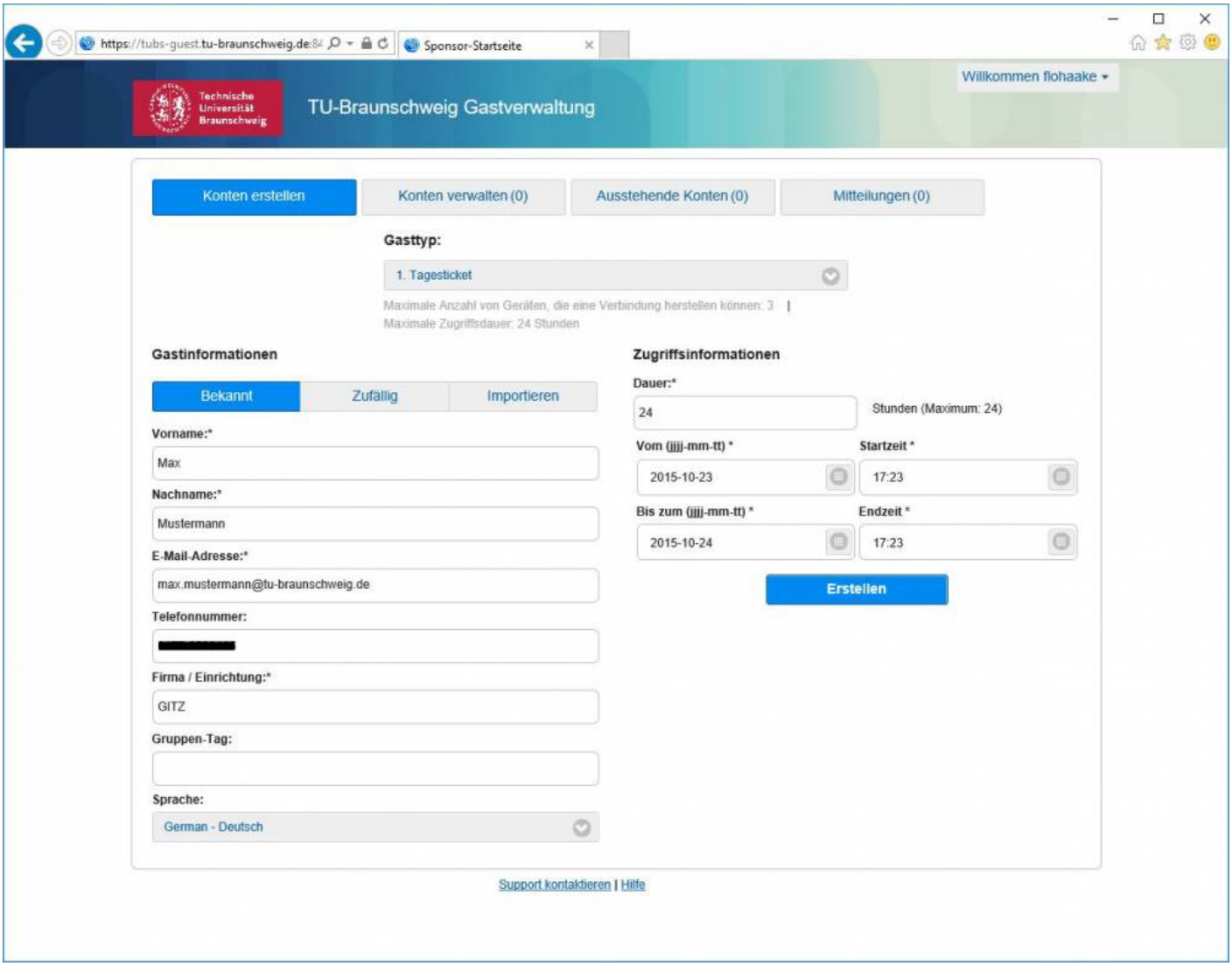
Bei Wochentickets erhält der „Ticketbesitzer“ einen Tag vor Ablauf eine E-Mail mit einem entsprechenden Hinweis. Bei Monatstickets erfolgt ein entsprechender Hinweis per E-Mail eine Woche und bei Quartalstickets 14 Tage vor Ablauf des Zugangs.

Maximale Anzahl von Geräten mit einer Gastkennung

Es können **maximal fünf** unterschiedliche Geräte zeitgleich mit einem Login verwendet werden. Dies ermöglicht z.B. die gleichzeitige Nutzung eines Notebooks, eines Tablets und drei weiteren Geräten.

Personalisierte Gast-Kennung erstellen (Reiter „Bekannt“)

Nach erfolgreichem Login wählen Sie in der Startansicht den Menüpunkt „Konto erstellen“ und „Bekannt“.



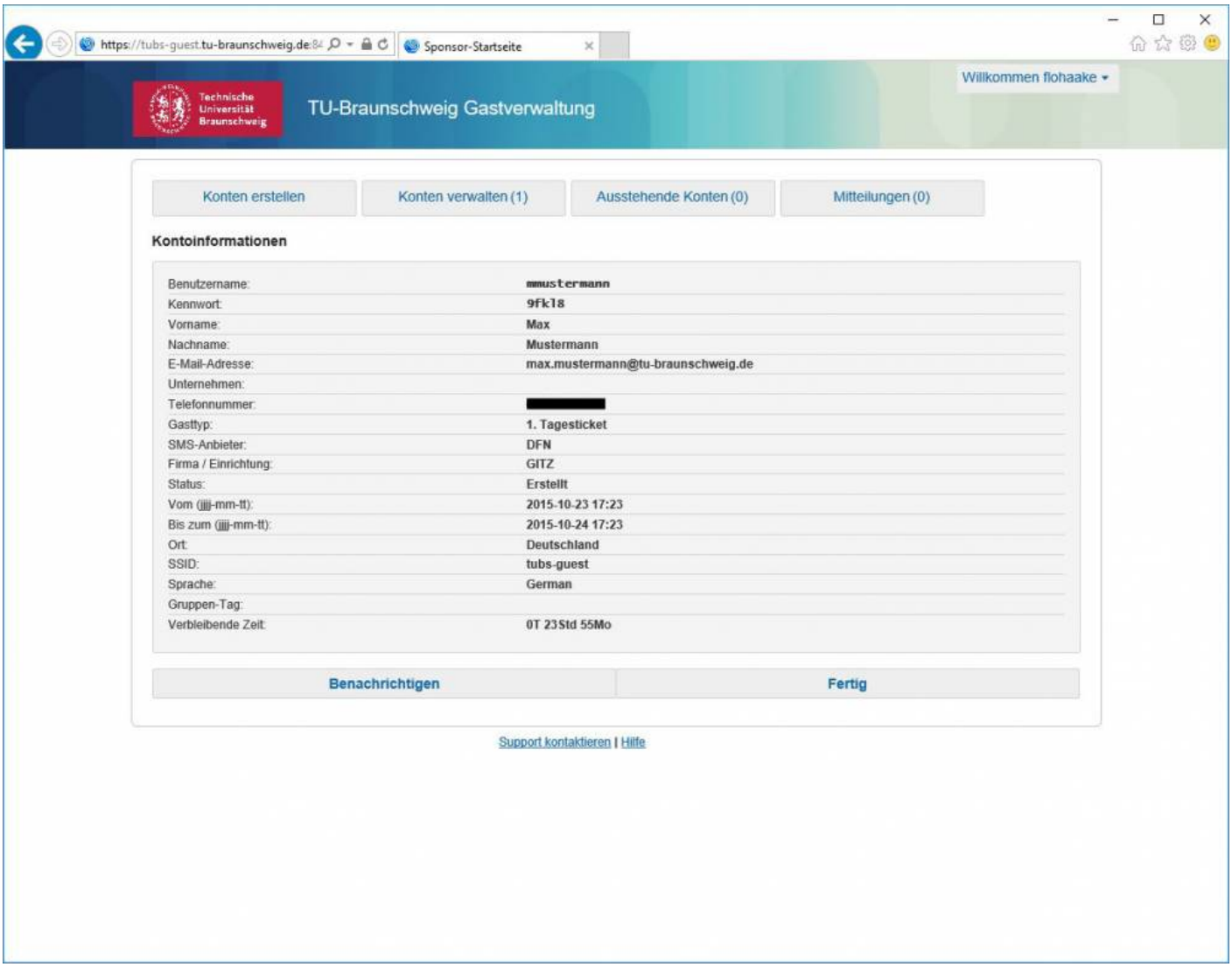
Es erscheint das abgebildete Fenster. Dort wird Vorname, Nachname, E-Mail-Adresse, Telefonnummer sowie Firma/Einrichtung angegeben. Der Gruppen-Tag dient der internen

Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.

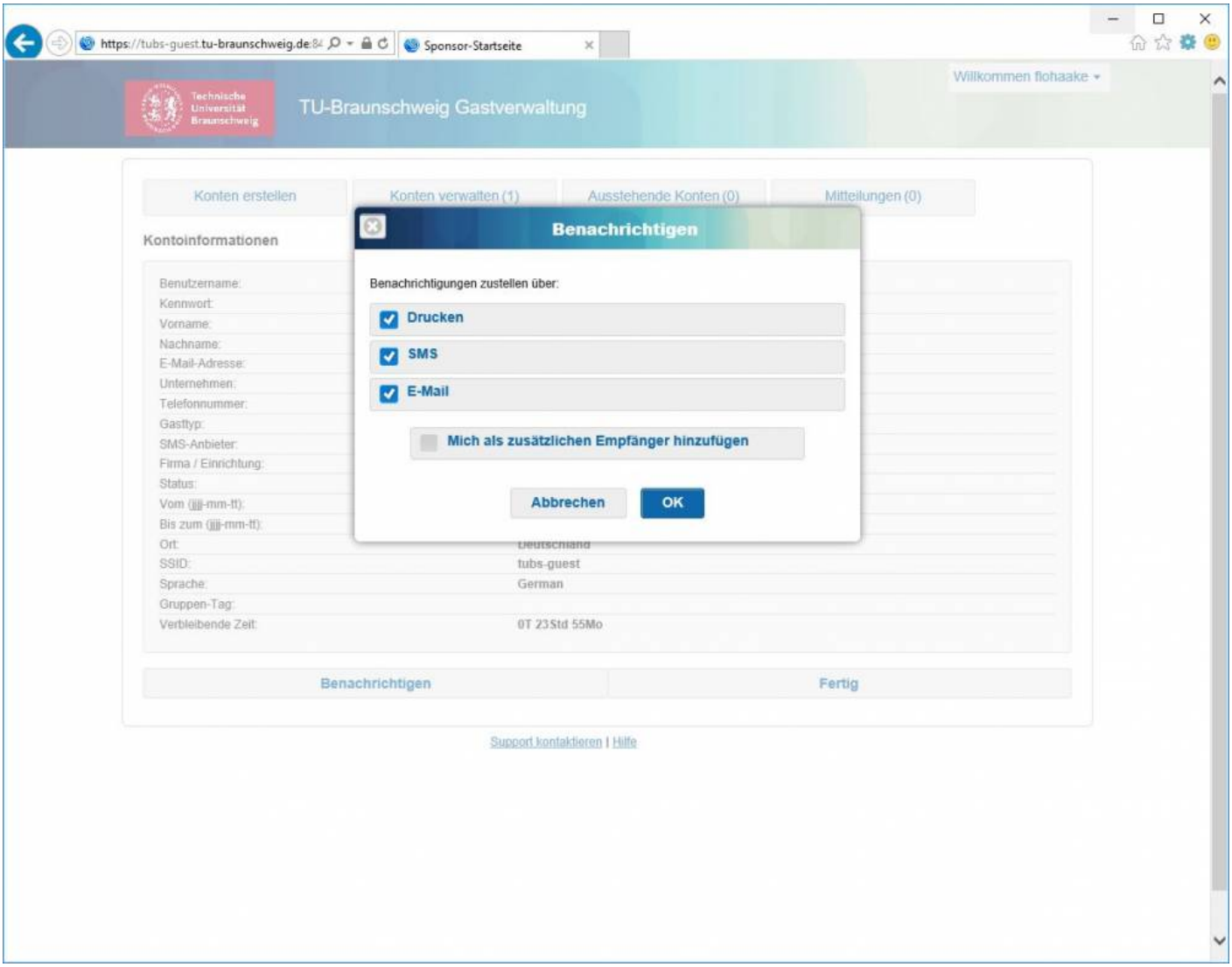
Es existieren zeitliche Beschränkungen für das Anlegen einer Gast-Kennung. Sowohl das Anlegen im Vorfeld als auch die maximale Nutzungsdauer sind befristet, siehe Abschnitt Zeitprofile. Sie können den Zeitraum flexibel per Hand eintragen oder die vordefinierten Zeitprofile verwenden.

Die mit (*) gekennzeichneten Attribute sind verpflichtend anzugeben.

Nach Erstellen der Gast-Kennung über [**Erstellen**] werden in der Übersicht die Details der Gast-Kennung angezeigt.

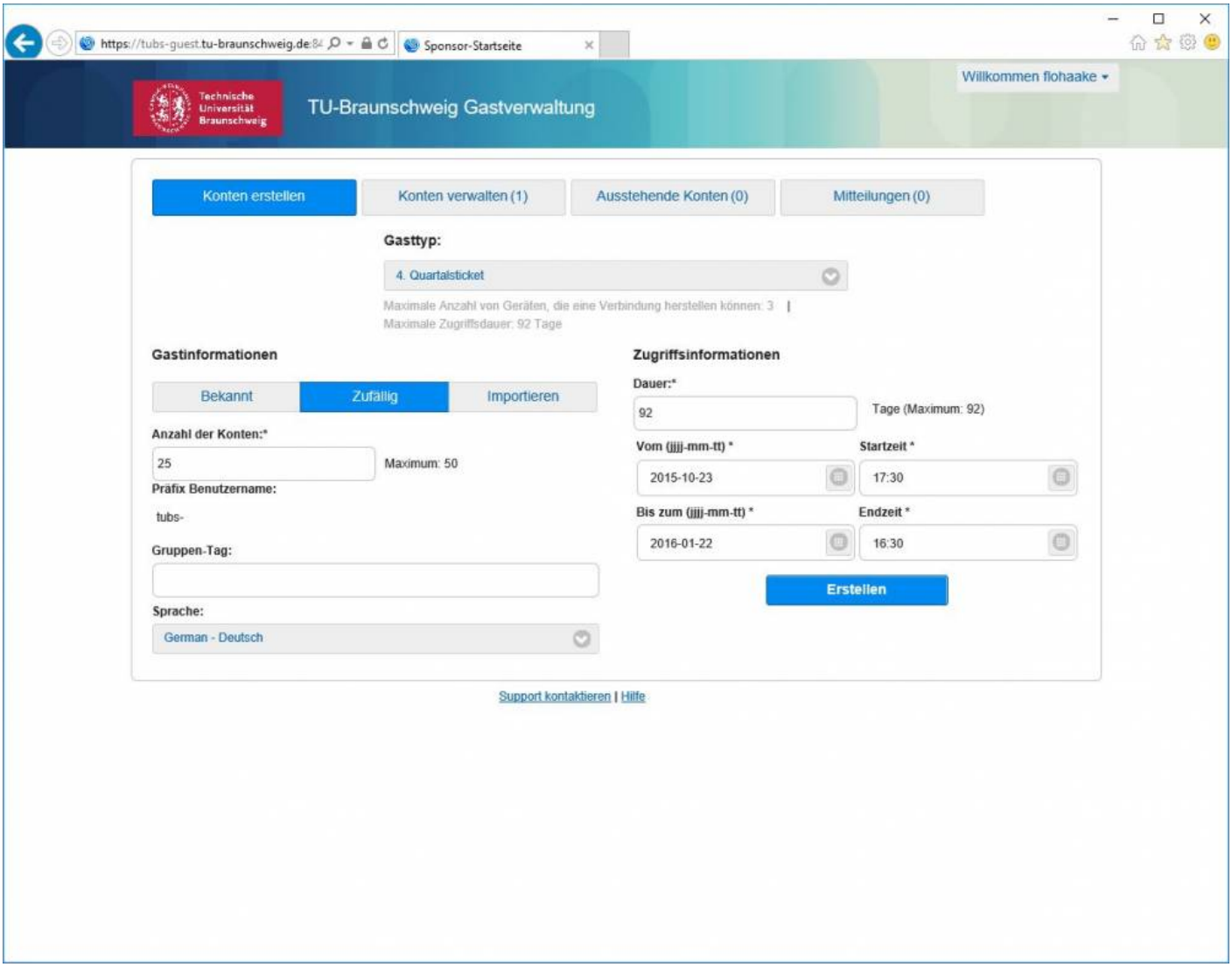


Es ist möglich die mit der Kennung verbundenen Zugangsdaten mit Benutzeranleitung auszudrucken oder/und an die angegebene E-Mail-Adresse zu versenden.



Mehrere Gast-Kennungen erstellen (Reiter „Zufällig“)

Nach erfolgreichem Login wählen Sie in der Startansicht den Menüpunkt „Konto erstellen“ und „Zufällig“ aus.



Sie können maximal bis zu 50 Benutzerkonten auf einmal anlegen. Nach einem Klick auf [**Erstellen**] haben Sie über die Funktion „Drucken“ die Möglichkeit sich eine PDF mit allen Kennungen (eine Seite pro Kennung) anzeigen zu lassen.

Bitte beachten Sie dass Systembedingt maximal 50 Gastaccounts in einem Vorgang erzeugt werden können, dieser Vorgang kann aber beliebig oft wiederholt werden. Wenn Sie für eine Veranstaltung mehr als 100 Accounts erzeugt haben oder benötigen, wenden Sie sich bitte mit dem Kontaktformular an die Abteilung Netze, damit eine ausreichende Versorgung mit W-LAN bereitgestellt werden kann für ihre Veranstaltung.

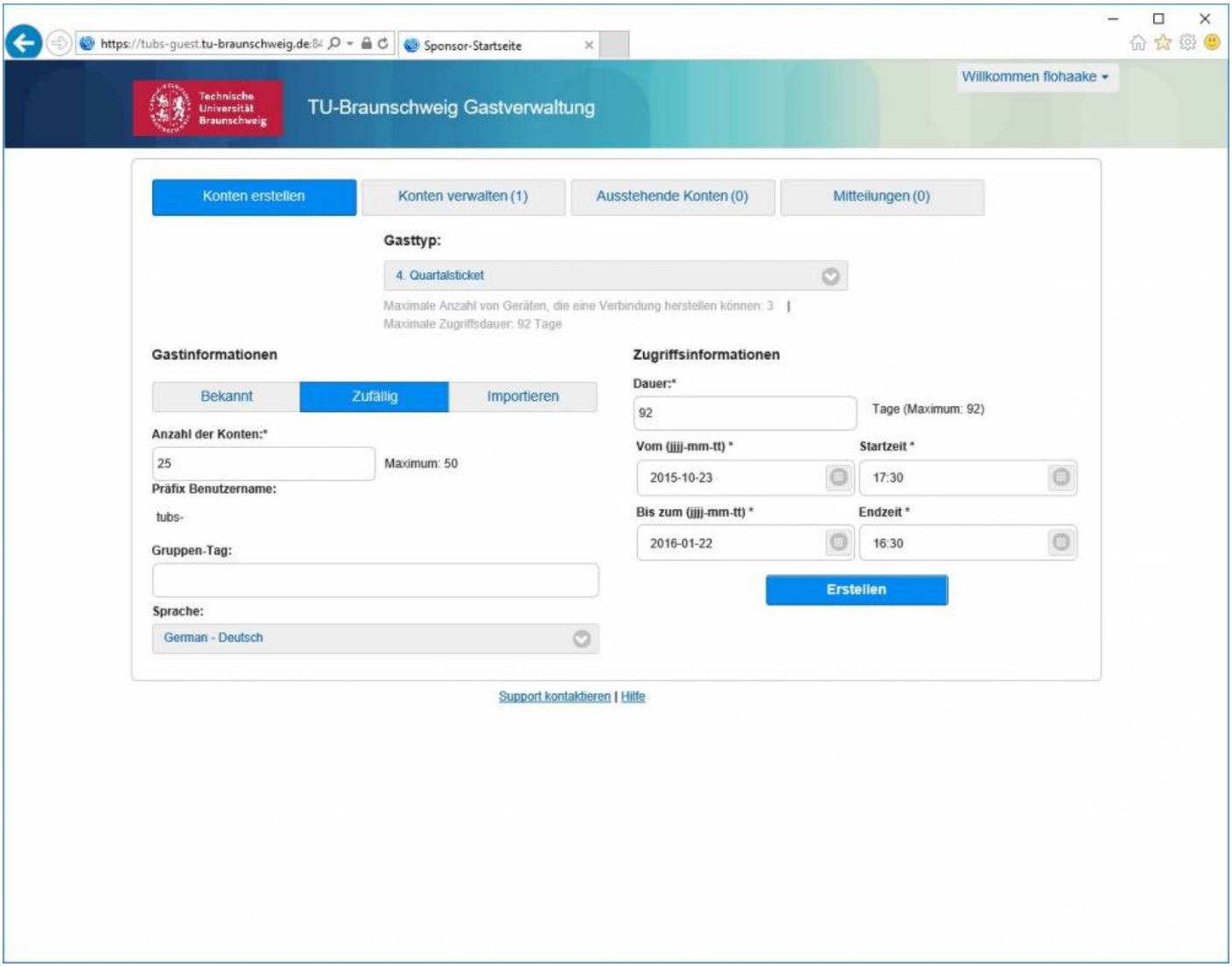
Die mit (*) gekennzeichneten Attribute sind verpflichtend anzugeben. Der Gruppen-Tag dient der internen Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.

Es existieren zeitliche Beschränkungen für das Anlegen einer Gast-Kennung. Sowohl das Anlegen im Vorfeld als auch die maximale Nutzungsdauer sind befristet, siehe Abschnitt Zeitprofile.

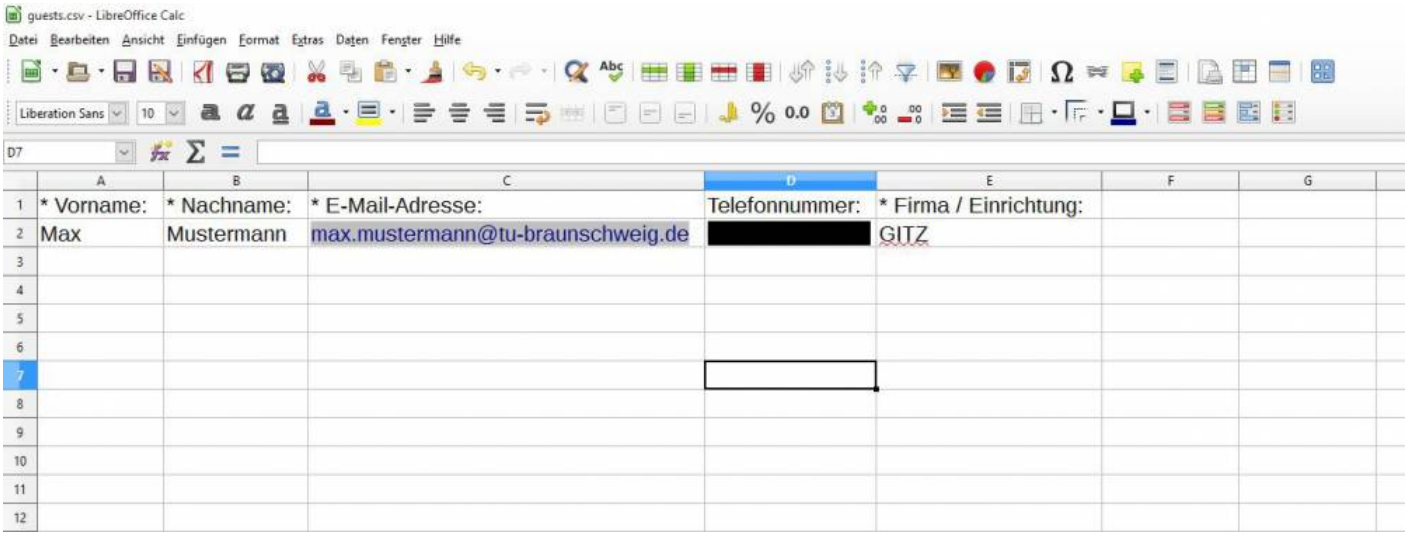
Bei der Ausgabe von nicht personalisierten Gast-Kennungen ist darauf zu achten, dass diese bei der Ausgabe personalisiert werden. Auf dem Ausdruck finden Sie einen Abschnitt, den Ihre Gäste vollständig ausfüllen müssen. Die Hinweise aus dem Abschnitt Aufzeichnungspflichten müssen Sie beachten.

Mehrere Gast-Kennungen via CSV-Datei importieren (Reiter „Importieren“)

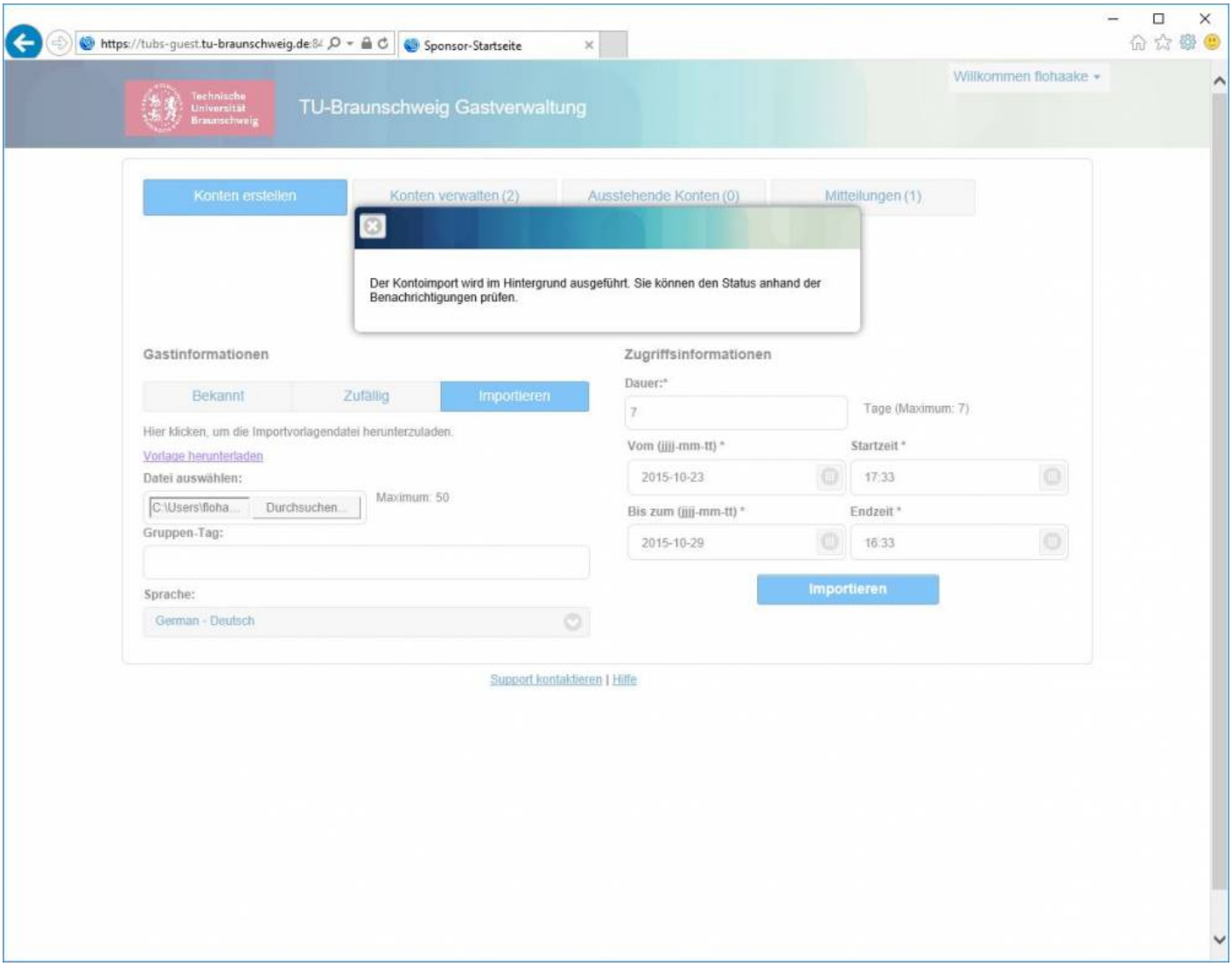
Über diese Funktion haben Sie die Möglichkeit eine CSV-Datei mit bis zu 50 Gast-Benutzern zu importieren und entsprechend Kennungen generieren zu lassen. Ein Beispiel für die Formatierung der CSV-Datei können Sie über „Vorlage herunterladen“ direkt auf Ihrem Computer speichern. Wir empfehlen die Nutzung dieser Vorlage.



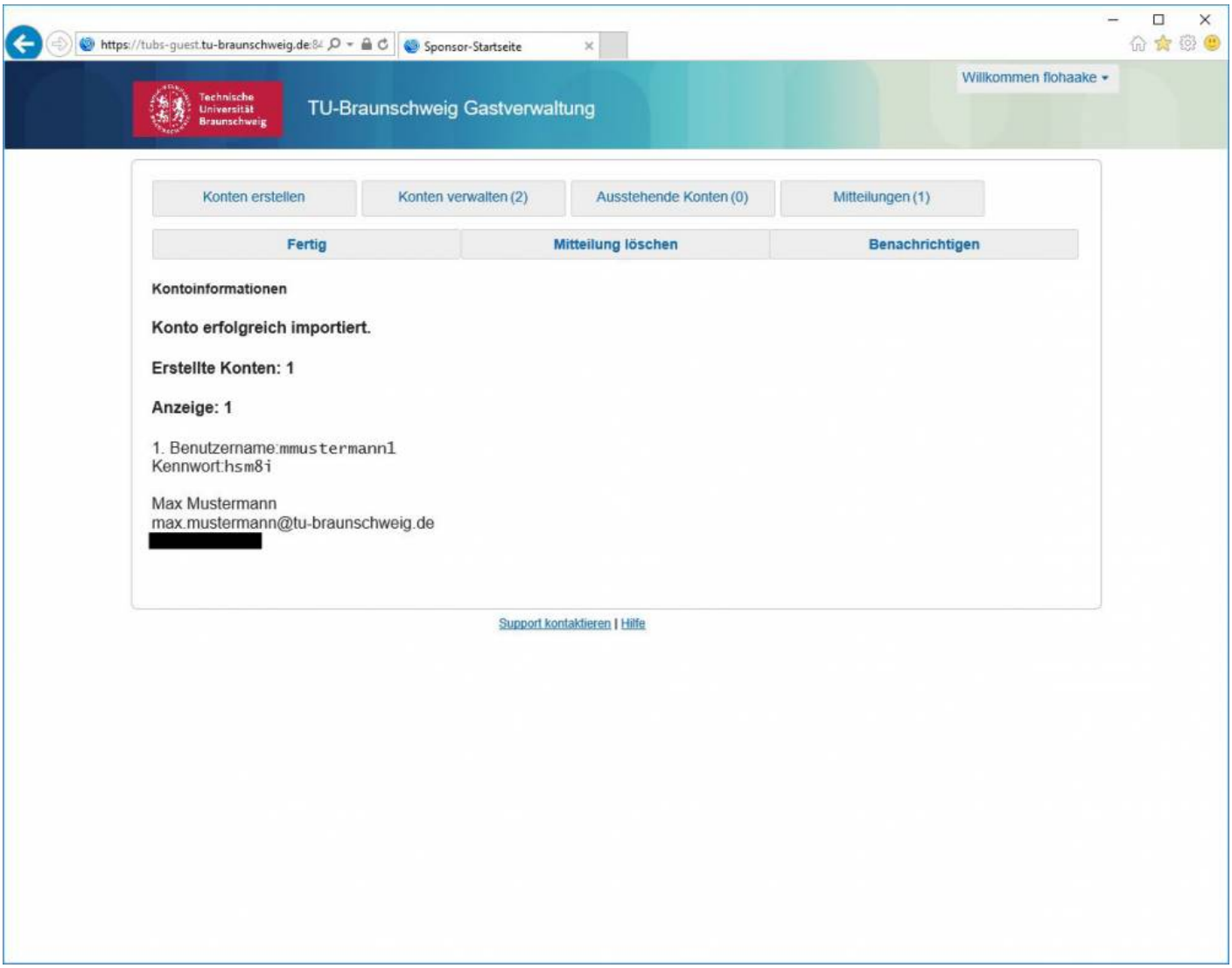
Die mit (*) gekennzeichneten Attribute in der CSV-Datei sind verpflichtend anzugeben. Als Trennzeichen wir das Komma benutzt um die Felder in der CSV-Datei zu trennen. Ein anderes Zeichen als Trennzeichen zu benutzen führt zu einem Fehler. Der Gruppen-Tag dient der internen Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.



Nach Auswahl und Upload der CSV-Datei werden die angeforderten Gast-Kennungen im Hintergrund generiert.

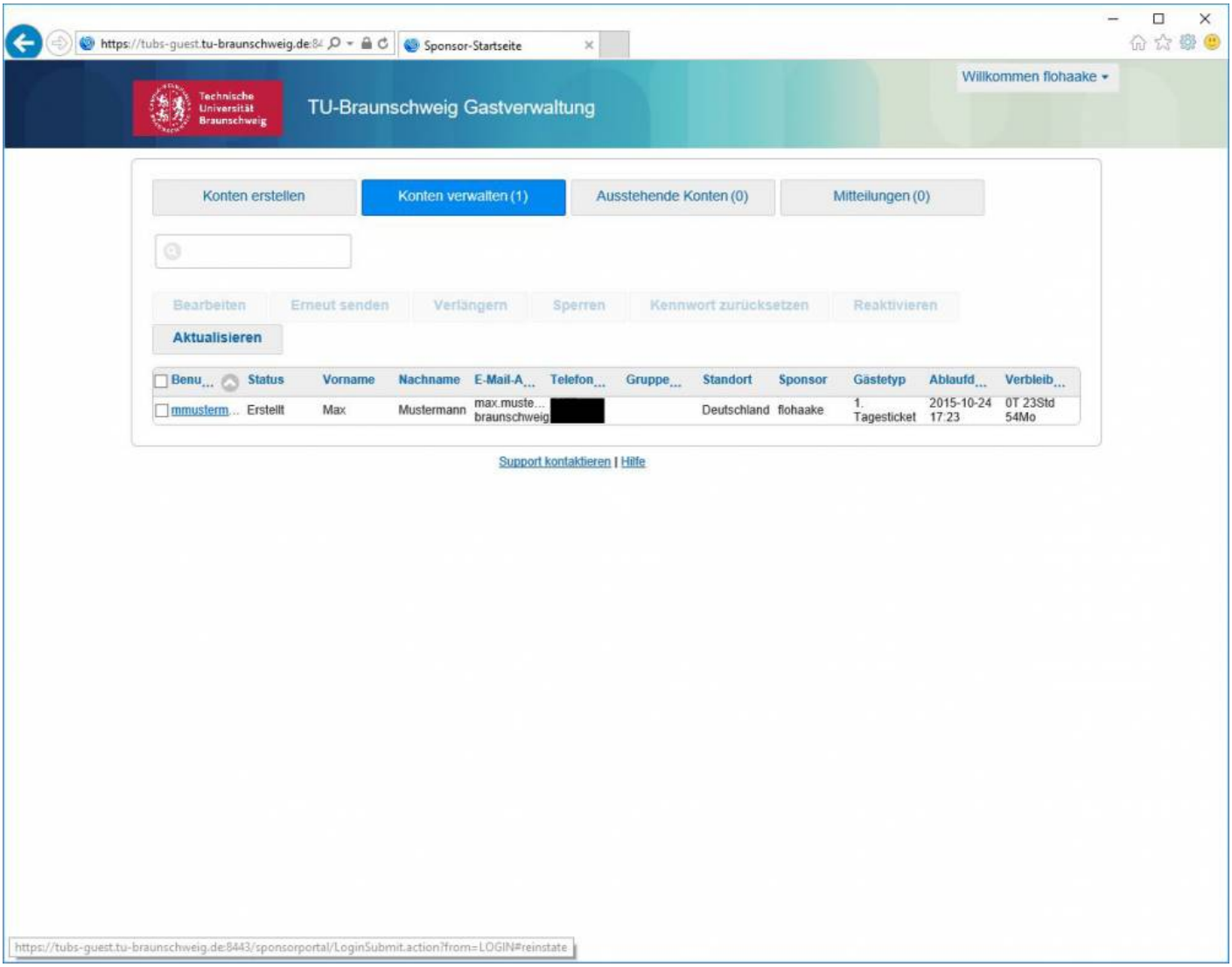


In dem Menüpunkt „Mitteilungen“ finden Sie nach Fertigstellung eine neue Nachricht mit den erzeugten Kennungen. Über „Benachrichtigen“ können Sie hier wie gewohnt eine PDF-Datei mit allen Gast-Kennungen inkl. Anleitungen generieren sowie die Nutzer per E-Mail.



Verwalten von Gast-Kennungen

Über den Menüpunkt „Konten verwalten“ haben Sie die Möglichkeit bestehende Gast-Kennungen zu verwalten bzw. zu editieren.



- [**Bearbeiten**]: Nachträgliches Editieren der Kontaktdaten des Gastes
- [**Erneut senden**]: Zugangsdaten erneut versenden/ausdrucken
- [**Verlängern**]: Gast-Kennung um maximal 24 Stunden verlängern
- [**Sperren**]: Gast-Kennung mit sofortiger Wirkung sperren
- [**Kennwort zurücksetzen**]: Passwort neu setzen und per E-Mail versenden / ausdrucken
- [**Reaktivieren**]: Konto wieder freischalten (nach Sperrung)

Verwaltung und Dokumentation von Gast-Kennungen

Die Verwaltung und Ausgabe von Gast-Kennungen erfolgt ausschließlich durch die zuständigen DV-Koordinatorinnen und DV-Koordinatoren der Institute und Einrichtungen.

Gast-Kennungen müssen spätestens bei ihrer Ausgabe eindeutig einer Person zugeordnet werden. Nicht personalisierte Gast-Kennungen sowie Sammelkennungen sind nicht zulässig. Die Weitergabe

von Gast-Kennungen an Dritte ist untersagt.

Die Personalisierung dient der sicheren Verwaltung der Zugangsberechtigungen und dem Schutz der universitären IT-Infrastruktur.

Die zuständigen DV-Koordinatorinnen und DV-Koordinatoren sind dafür verantwortlich, die Zuordnung zwischen Gast-Kennung und berechtigter Person nachvollziehbar zu dokumentieren.

Die Dokumentation kann elektronisch oder in Papierform erfolgen. Dabei dürfen ausschließlich die für die Verwaltung und Nachvollziehbarkeit der Zugangsberechtigungen erforderlichen personenbezogenen Daten erhoben und gespeichert werden.

Die personenbezogenen Daten sind vor unberechtigtem Zugriff zu schützen und entsprechend den geltenden Datenschutzbestimmungen sowie den festgelegten Aufbewahrungs- und Löschfristen zu löschen oder datenschutzgerecht zu vernichten.

Anfragen zur Zuordnung von Gast-Kennungen sind an das Gauß-IT-Zentrum zu richten. Die Weitergabe personenbezogener Daten an Ermittlungsbehörden oder andere externe Stellen erfolgt ausschließlich nach Prüfung der rechtlichen Voraussetzungen durch die zuständigen Stellen der Universität.

Die technische Bereitstellung, Deaktivierung und Löschung der Gast-Kennungen in den zentralen Systemen erfolgt durch das Gauß-IT-Zentrum.

Ausgabepraxis von Gast-Benutzerkennungen

Seitens des DFN existieren keine expliziten Empfehlungen zur Ausgabepraxis von personalisierten Gast-Benutzerkennungen. Auf Anfrage wurde mitgeteilt, dass eine Übergabe von personalisierten Gast-Benutzerkennungen gegen Empfangsquittung und persönlicher Identifizierung der empfangenden Person anhand eines gültigen amtlichen Lichtbildausweises die haftungsrechtlich unbedenklichste Lösung ist. Abstriche an diesen hohen Anforderungen lassen das Haftungsrisiko aufgrund möglicher missbräuchlicher Nutzung steigen.

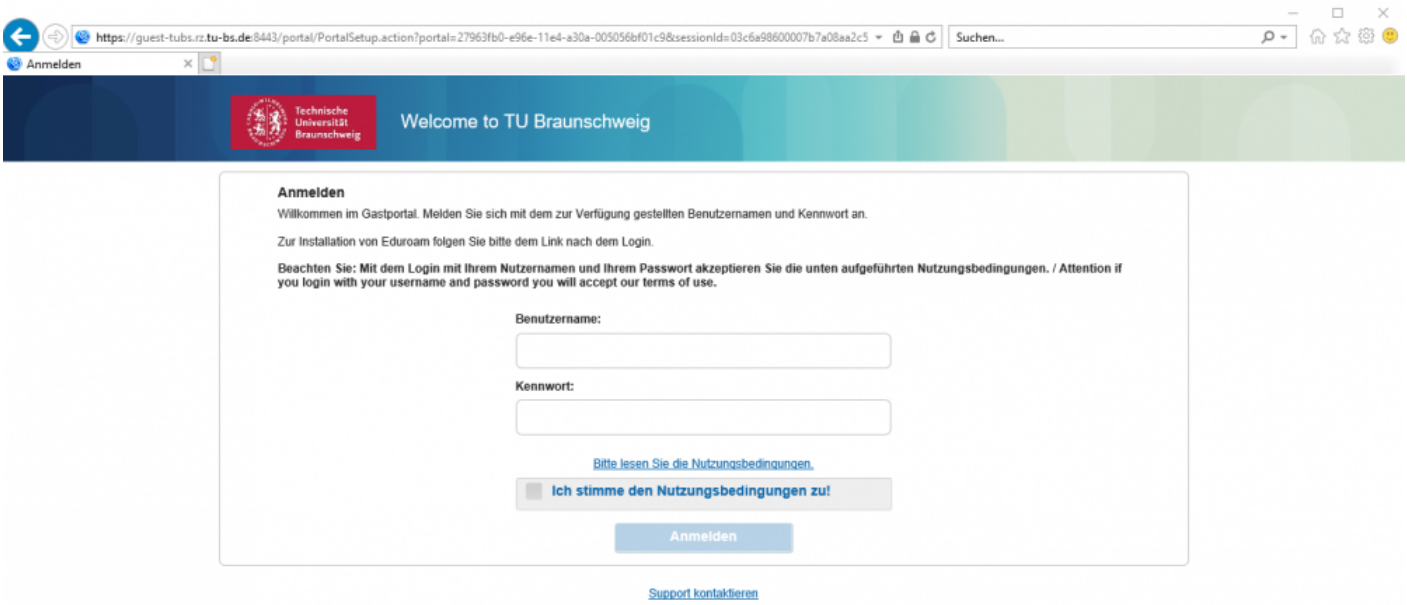
Welchen Grad erhöhter Haftungsrisiken Institute oder Einrichtungen bereit sind zu tragen, obliegt ihnen selbst. Eine Risikoabschätzung muss individuell erfolgen. Seitens des DFN können daher keine verbindlichen Empfehlungen gegeben werden. Als Hinweis zur Abschätzung wird jedoch wie folgt erläutert: Tritt ein Fall von missbräuchlicher Nutzung einer Gast-Benutzerkennung ein und wird dieser Missbrauch durch Polizei und Staatsanwaltschaft geahndet, so ist das Institut/die Einrichtung, die den Zugang durch Erstellen und Ausgabe der Gast-Benutzerkennung gewährt hat, in der Nachweispflicht an wen konkret die Gast-Benutzerkennung ausgegeben worden ist.

In einem Ermittlungsverfahren werden Polizei und Staatsanwaltschaft dann gegen die genannte Person ermitteln. Kann das Institut/die Einrichtung diesen Nachweis nicht erbringen oder werden die vorgelegten Nachweise im Strafverfahren vom Gericht als nicht ausreichend angesehen, so kann dann der Fall einer Mitstörerhaftung eintreten. Handreichung für eine praktikable Umsetzung passend zu Risikoabschätzung in Ihrer Einrichtung: Von Aushändigung gegen Vorlage der persönlichen Konferenzeinladung am Konferenzdesk - so wie es auch an anderen Einrichtungen üblich ist - bis Versand an die bei der Konferenzanmeldung und Zahlung der Konferenzgebühr übermittelten Post- oder E-Mail-Adresse sind verschiedene Optionen denkbar, die Sie ggf. mit der Leitung Ihres Instituts oder Einrichtung abstimmen.

Als Information für Ihren Abwägungsprozess sei angemerkt, dass die Mehrzahl der Meldungen durch das DFN-CERT erfolgen und lediglich auf kompromittierte Rechner hinweisen (einige Hundert). Gelegentlich finden allerdings auch Ermittlungsanfragen von Polizei und Staatsanwaltschaft statt.

Nutzung durch Gäste

Nachdem Sie über die Selbstbedienungsschnittstelle Gast-Benutzerkennungen generiert haben, erhalten die Nutzer ihre Zugangsdaten mit Benutzeranleitung per E-Mail oder entsprechend durch Sie ausgehändigt. Die Nutzung durch Ihre Gäste ist weitgehend selbsterklärend und intuitiv. Gäste können ihre Geräte über das WLAN-Netz (SSID) tubs-guest verbinden. Der Einsatz verschlüsselter Protokolle wie HTTPS, IMAPS, VPN, usw. oder/und VPN werden empfohlen. Nach erfolgreicher Verbindung mit tubs-guest werden alle (http-)Aufrufe im Internetbrowser automatisch auf eine TLS-gesicherte Login-Seite umgeleitet. Um das Internet nutzen zu können, müssen die Gäste die erhaltenen Zugangsdaten eingeben und die Nutzungsbedingungen akzeptieren.



Created 2024-02-28 11:16:15 UTC by Nils Koschnitzki
Updated 2026-11-12 17:42:59 UTC by Nils Koschnitzki