Anmeldevorgang Webmail (OWA)

Um sich bei der Webmail anmelden zu können, benötigen Sie ihr persönliches Datenblatt bzw. die folgenden Daten:

Benutzer-/Anmeldenamen
Passwort
Schlüssel der 2-Faktor-Authentifizierung

Für die 2-Faktor-Authentifizierung benötigen Sie den Google-Authenticator auf Ihrem Smartphone oder Mobile Device (s. Anleitung ab Seite 3).

Login in Outlook Web Access (OWA)

Öffnen Sie auf Ihrem Endgerät ein Browserfenster (Internetexplorer, Firefox, Chrome, usw.) und geben Sie die Web-Adresse https://mail0001.rlp.cloud ein. Sie sollten diese Seite in den Favoriten abspeichern.

Hier geben Sie bitte in das Feld „Benutzername" ihren Benutzer-/Anmeldenamen in der Schreibweise wie auf dem persönlichen Datenblatt angegeben und unter „2-Faktor" das One-time Passwort, dass Sie auf Ihrem mobilen Gerät ablesen, ein. Betätigen Sie zeitnah die Schaltfläche ***Absenden*** (Abbildung 1).

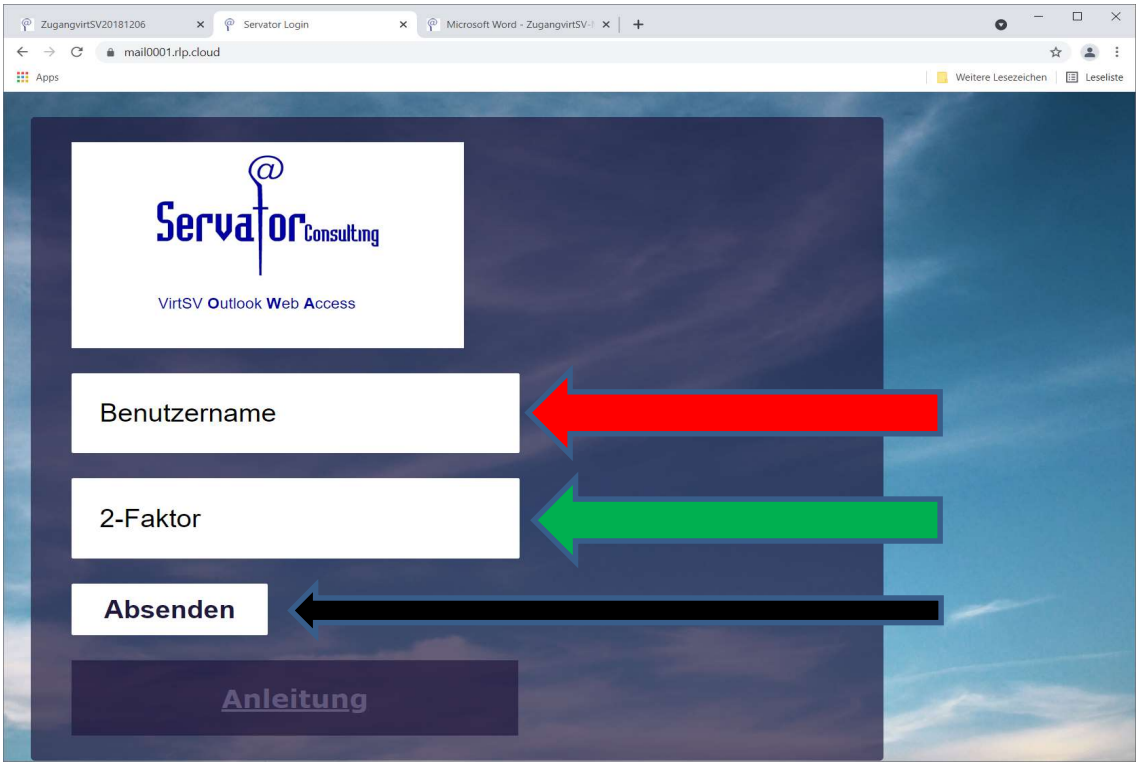

Abbildung 1

Die Systemuhr auf dem lokalen PC muss die korrekte Uhrzeit haben, da das generierte One-time Passwort sonst nicht angenommen wird!

Nach der erfolgreichen Authentifizierung erhalten Sie das Anmeldefenster für den Outlook Web Access (s. Abbildung 2).

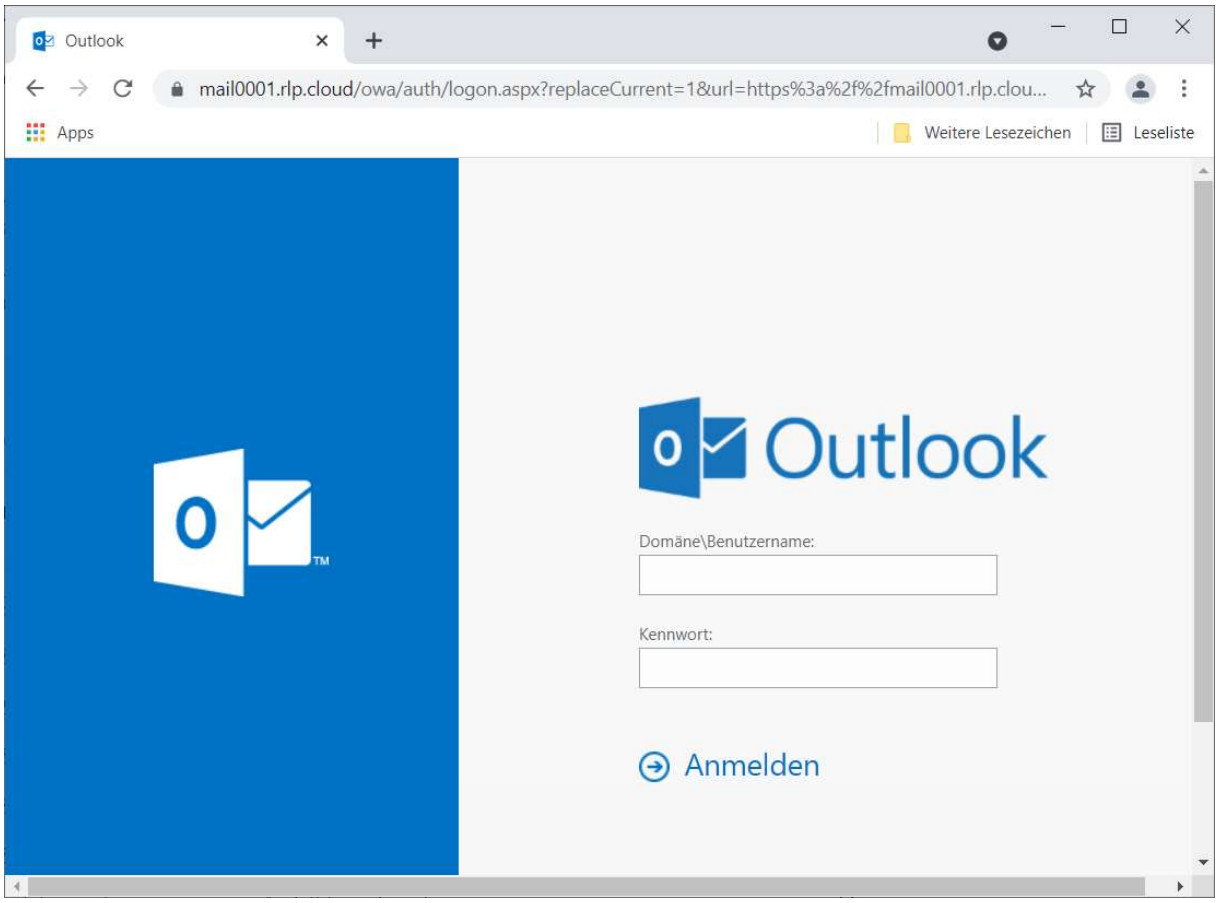

Abbildung 2

Hier geben Sie bitte in das Feld „Domäne\Benutzername:" den Domänennamen, einen Backslash („\") und Ihren Benutzer-/Anmeldenamen ein.

Der aktuelle Domänenname lautet **virtsv0001**.

Beispiel: virtsv0001\R12345-AbcdE

Danach geben Sie im Feld „Kennwort:" Ihr persönliches Passwort ein.

Nach der Bestätigung mit ***Anmelden*** haben Sie Zugriff auf Ihr Postfach.

Installation und Einrichtung des Google Authenticator

Diese Anleitung beschreibt die Installation und Einrichtung des Google-Authenticator für Android.

Sollten Sie keinen Google-Authenticator verfügbar haben, so können Sie auch über die Web-Adresse https://secure.servator.de die notwendigen Schritte ausführen (s. Beschreibung am Ende).

Rufen Sie den Google Play Store auf Ihrem Mobilgerät auf (Abbildung 1).
Geben Sie im Suchfeld ***Google Authenticator*** ein (Abbildung2).
Betätigen Sie die Schaltfläche ***Installieren*** (Abbildung 3).

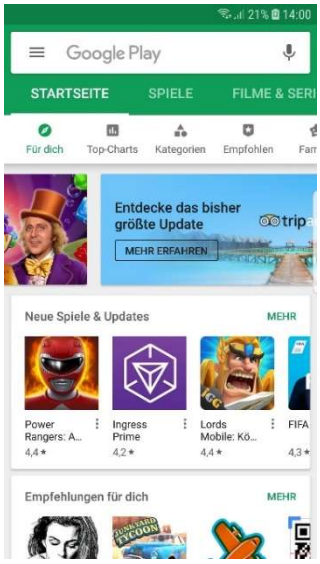

Abbildung 1

Abbildung 2

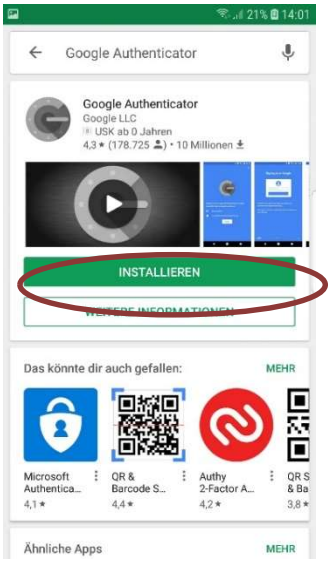

Abbildung 3

Beachten Sie, dass aus Sicherheitsgründen die Nutzung eines Smartphones oder anderen Mobile Device für den Google-Authenticator empfohlen wird, bzw. ein Gerät für die Google-Authentication verwendet werden sollte, mit dem Sie sich **nicht** zeitgleich in die Webmail einloggen.

Die Software Google-Authenticator wird installiert (Abbildung 4).
Nach Abschluss der Installation ***Öffnen*** sie die Anwendung (Abbildung 5)
und betätigen die Schaltfläche ***Starten*** (Abbildung 6).

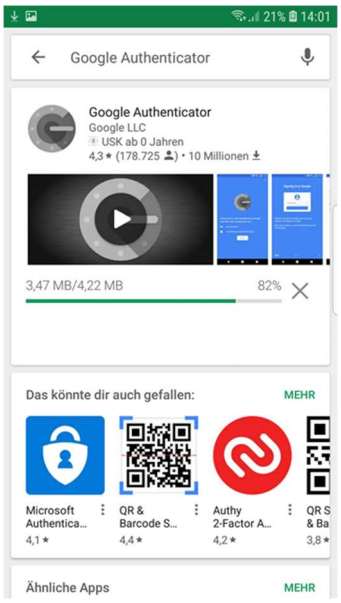

Abbildung 4

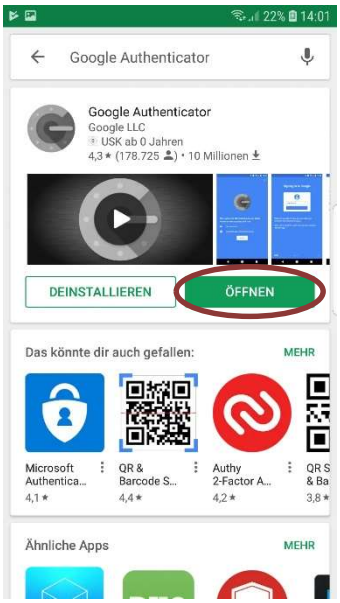

Abbildung 5

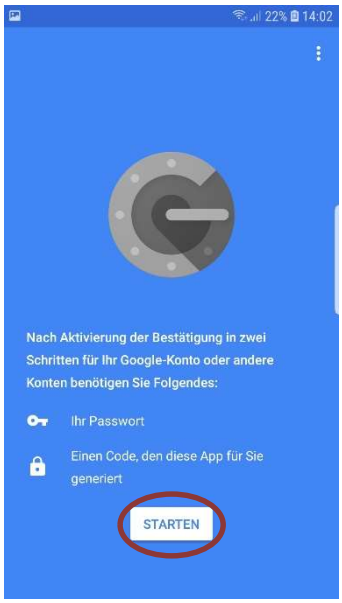

Abbildung 6

Wählen Sie ***Schlüssel eingeben***, um ein Konto hinzuzufügen (Abbildung 7).

Für die Eingabe der Kontodaten benötigen Sie den Benutzer-/Anmeldenamen und den Schlüssel der 2-Faktor-Authentifizierung.

Geben Sie im Feld Kontoname Ihren Benutzer-/Anmeldenamen ein (Abbildung 8).
Geben Sie im Feld Mein Sicherheitsschlüssel Ihren Schlüssel der 2-Faktor-Authentifizierung ein und betätigen Sie die Schaltfläche ***Hinzuf.*** (Abbildung 9).

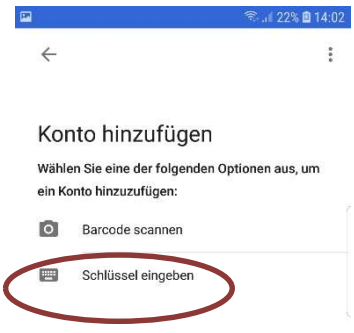

Abbildung 7

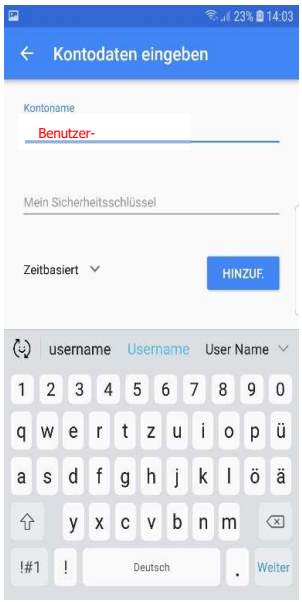

Abbildung 8

Abbildung 9

Nach dem das Konto hinzugefügt wurde erscheint eine 6-stellige Kombination, das One-time Passwort, der zugehörige Benutzer-/Anmeldename wird angezeigt (Abbildung 10).

Dieses ist jeweils für 2 Minuten gültig und ändert sich nach dieser Zeit.

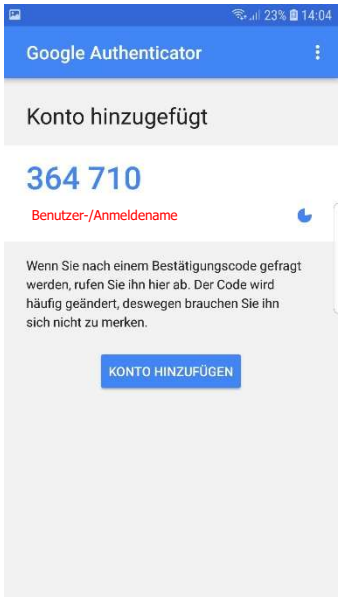

Abbildung 10

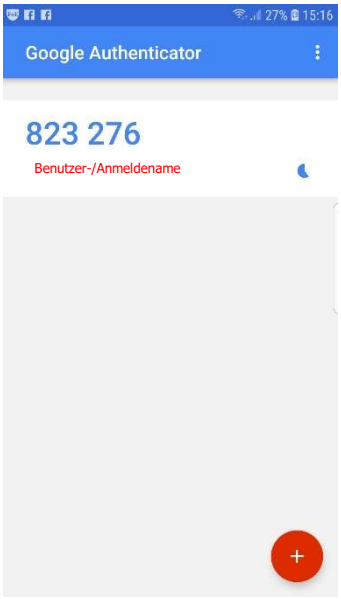

Abbildung 11

Wird die Anwendung Google-Authenticator zukünftig gestartet, kann man das aktuelle One-time Passwort sofort ablesen (Abbildung 11).

Anmeldung ohne Google-Authenticator

Öffnen Sie ein Browserfenster (Internetexplorer, Firefox, Chrome, usw.) und geben Sie die Web-Adresse https://secure.servator.de ein.

In diesem Fenster geben Sie bitte unter „Benutzer" ihren Benutzer-/Anmeldenamen in der Schreibweise wie auf dem persönlichen Datenblatt angegeben ein und im Feld „Schlüssel" den Schlüssel der 2-Faktor-Authentifizierung.

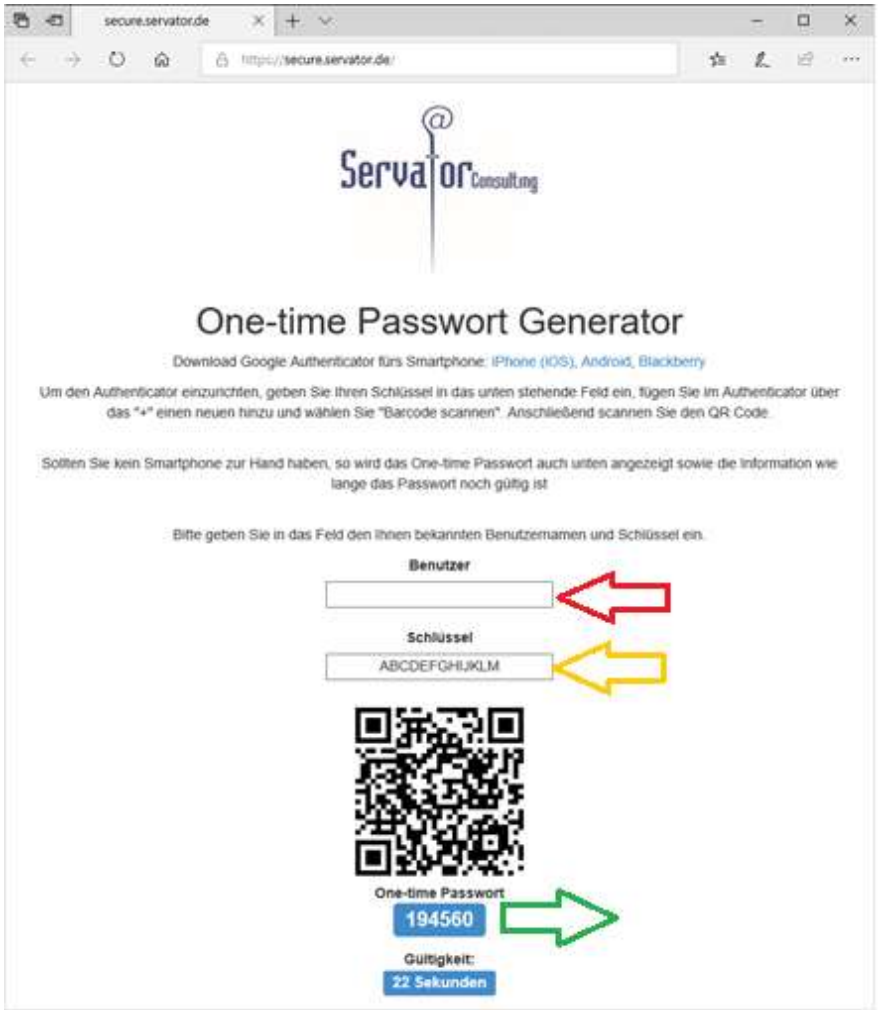

Abbildung 12: Generierung des One-time Passworts über Browserfenster

Daraus wird ein sechsstelliges One-time Passwort generiert, das jeweils für 2 Minuten gültig ist. Nach Ablauf der Gültigkeit wird sofort ein neues Passwort generiert.

Beachten Sie, dass aus Sicherheitsgründen die Nutzung eines Smartphones oder anderen Mobile Device für den Aufruf der Webseite empfohlen wird, bzw. ein Gerät für die Google-Authentication verwendet werden sollte, mit dem Sie sich nicht zeitgleich in die Webmail einloggen.