

E-Mail Verschlüsselung

Beschreibung der im Kispi eingesetzten Methode "PGP Universal Web Messenger"

Dokumentenversion 1.0

19. Oktober 2006

Autor: Informatik

Inhaltsverzeichnis

1.	PGP Universal Web Messenger	3
2.	Browser auf Empfänger Seite (PGP Universal Web Messenger).....	4
2.1	Versenden einer PGP Universal Web Messenger Einladung	4
2.2	Inbetriebnahme des Web Messenger Mailkontos durch den externen E-Mail-Empfänger	4
2.3	Testen des PGP Universal Web Messengers	7

1. PGP Universal Web Messenger

Den Kispi Mitarbeitern steht neu ein System zur Verschlüsselung von E-Mails zur Verfügung.

Ab sofort dürfen damit E-Mails, die Daten enthalten, welche der Datenschutzverordnung unterliegen (z.B. Patientendaten) autorisierten Empfängern zugestellt, bzw. von dort empfangen werden!

Die eingesetzte Methode ("PGP Universal Web Messenger"), welche nachstehend beschrieben wird, weist folgende Besonderheiten auf:

- Der E-Mail-Empfänger (z.B. ein Hausarzt) kann mit seinem **Internet Browser** auf eine verschlüsselte WEB-Seite auf einen KISPI Server (<https://kispiskey.unizh.ch>) zugreifen. Dieser Zugriff ist ebenfalls verschlüsselt.
- Der E-Mail-Empfänger kann sich auf dem oben erwähnten Kispi Server ein sicheres Mailkonto einrichten, über das er verschlüsselte Mails mit dem Kispi austauscht.
- Da das Mailkonto auf dem Kispi Server verwaltet wird, müssen E-Mails inkl. Anhänge (Beilagen) zur Weiterbearbeitung vom E-Mail-Empfänger auf seinen PC herunter geladen werden. Diese Verbindung ist verschlüsselt.

Die Verantwortung für den korrekten Einsatz des hier beschriebenen technischen Verfahrens zur sicheren Übermittlung von Daten per E-Mail liegt bei den Benutzern bzw. den Benutzerinnen .

Diese haben auch sicher zu stellen, dass der Adressat berechtigt ist, die übermittelten Daten zu lesen.

2. Browser auf Empfänger Seite (PGP Universal Web Messenger)

Das Kinderspital Zürich bietet den Benutzern eine einfache Möglichkeit mit externen Personen Dokumente per E-Mail sicher auszutauschen.



Die externen E-Mail-Empfänger benötigen auf ihrem Computer keine besondere Software! Sie können ihre Arbeit mit einem Browser (z.B. dem Internet Explorer) erledigen.

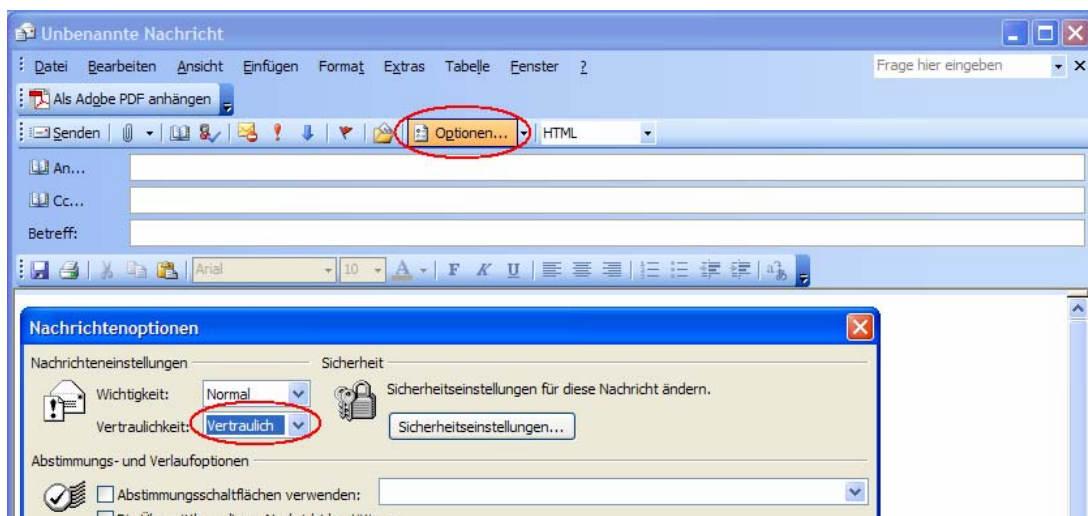
2.1 Versenden einer PGP Universal Web Messenger Einladung

Senden Sie Ihre E-Mail mit der "Option" **vertraulich** an den E-Mail-Empfänger. Mehr müssen Sie als Benutzer im Kinderspital nicht tun.

Der E-Mail-Empfänger erhält anschliessend vom Server eine PGP Universal Secure Message per E-Mail.



- Erstellen Sie ein neues Mail
- Wählen Sie "Optionen"
- **Setzen Sie das Feld "Vertraulichkeit:" auf "Vertraulich"**



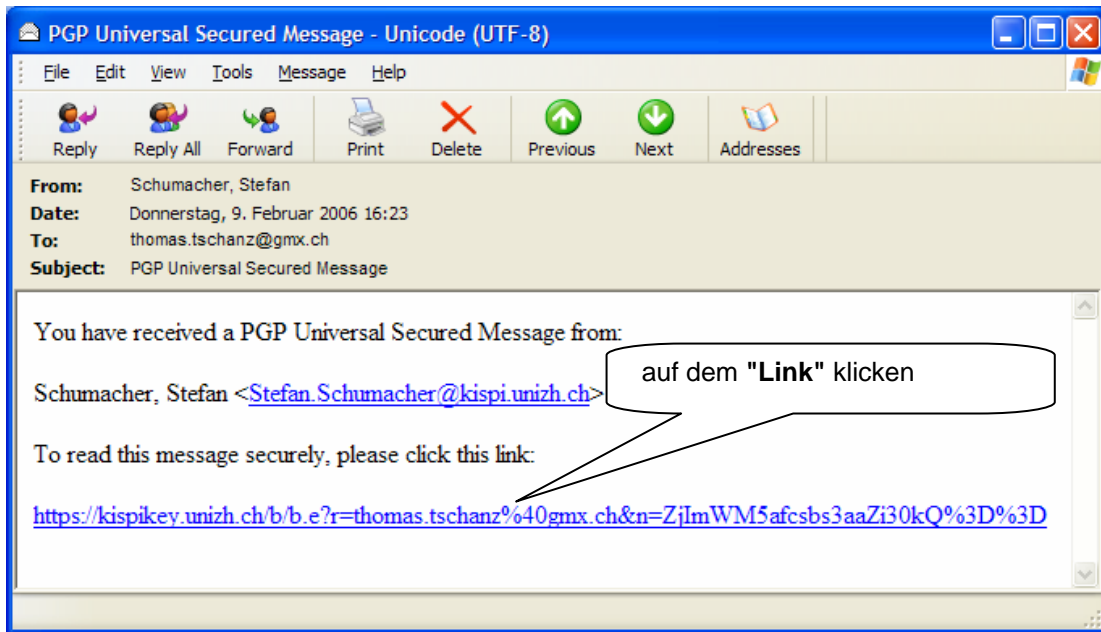
2.2 Inbetriebnahme des Web Messenger Mailkontos durch den externen E-Mail-Empfänger

Der E-Mail-Empfänger erhält anstatt des E-Mails eine PGP Universal Secure Message per E-Mail.

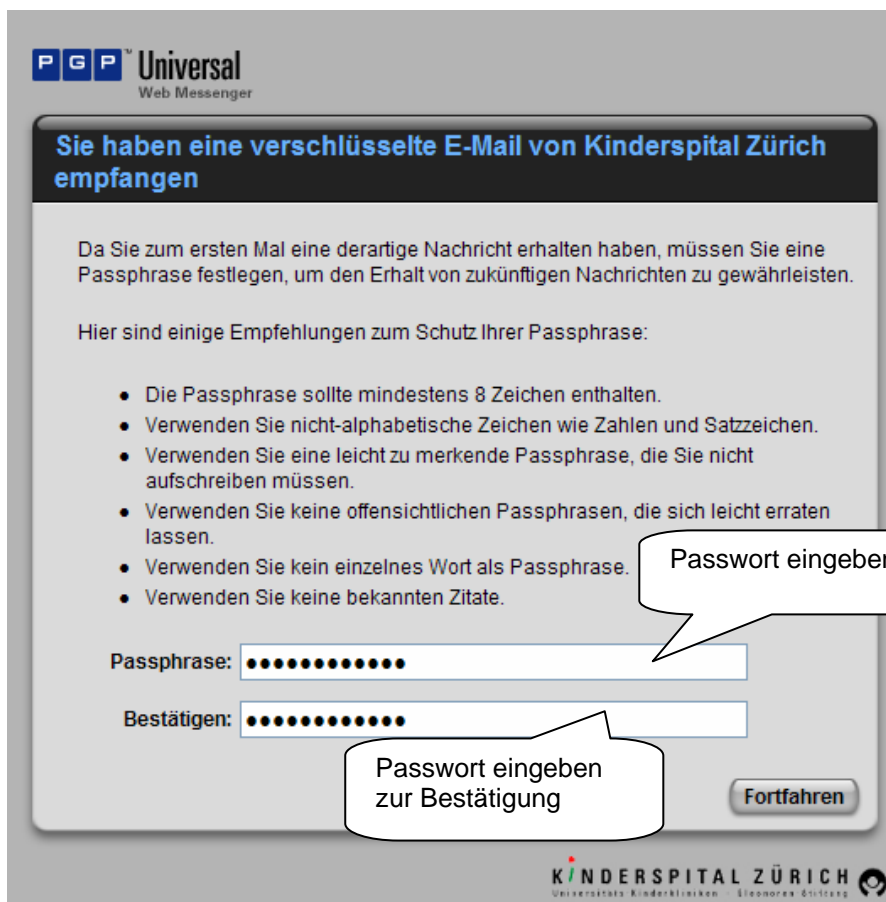


Mit einem **Mausklick** auf den Web-Link wird der E-Mail Empfänger auf den PGP Server im Kinderspital umgeleitet.

Achtung: Es kann auch sein, dass Sie den Web-Link in die Adresszeile des Browser kopieren müssen (abhängig vom Provider)!



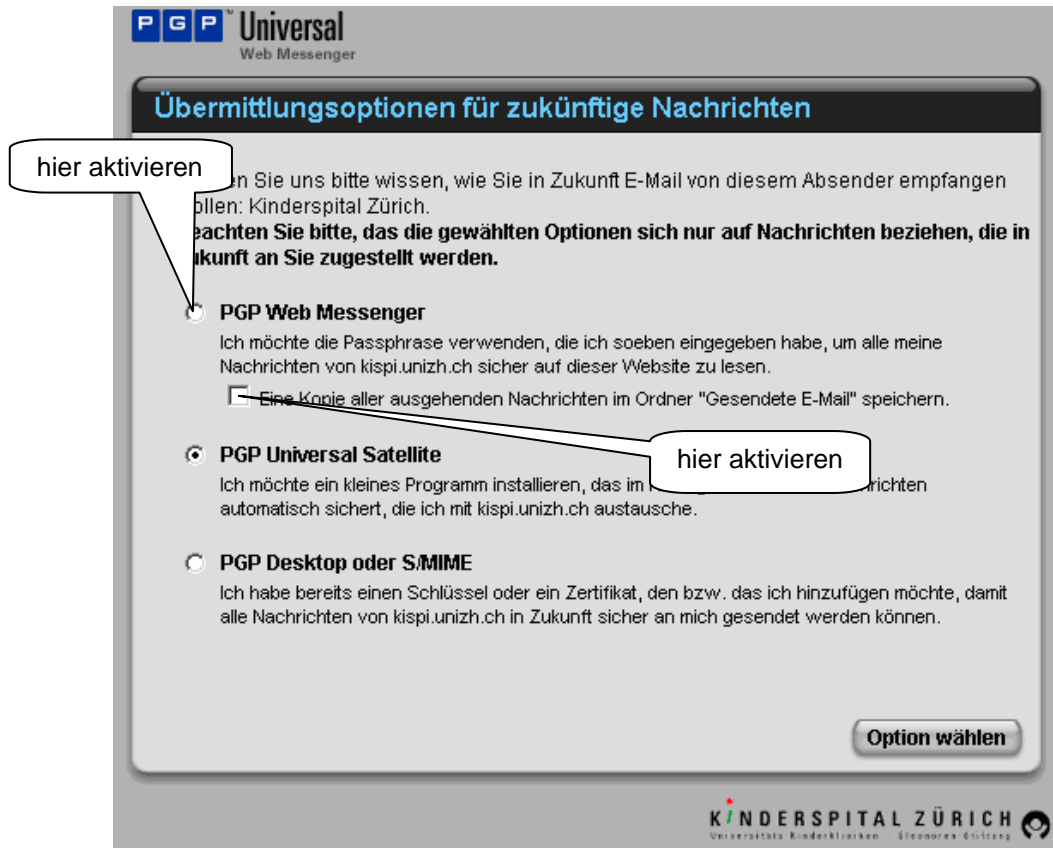
Nun wird der E-Mail-Empfänger **aufgefordert** ein **Passwort** (Passphrase) zu erstellen, welches er in Zukunft verwenden will.





Als letzter Schritt wird nun das **Web Messenger Mailkonto** (Postfach) **eingrichtet**.
 Dazu muss der E-Mail-Empfänger die folgenden zwei Optionen anklicken:

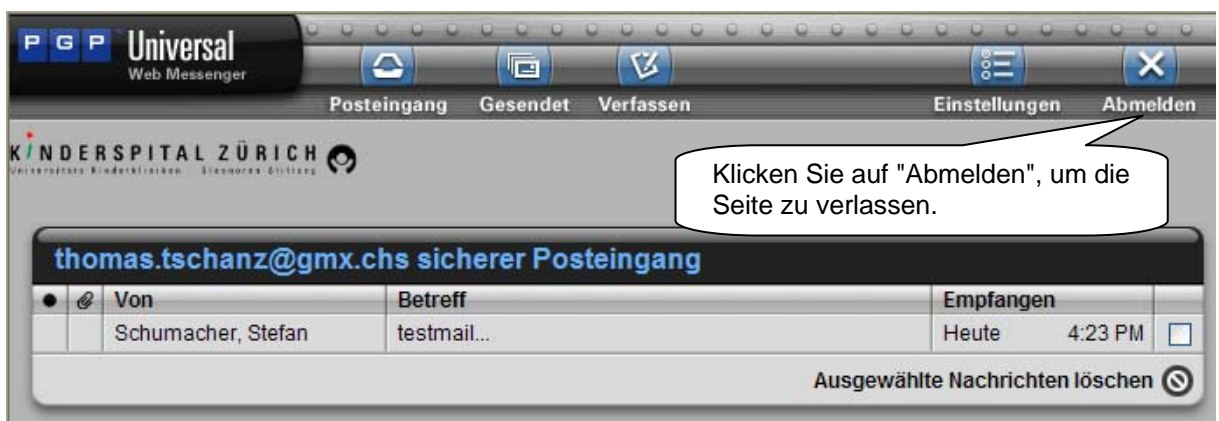
- PGP Web Messenger**
- Eine Kopie aller ausgehenden Nachrichten im Ordner gesendete E-Mail speichern**



Nun ist das sichere Mailkonto für den E-Mail-Empfänger fertig eingerichtet.



Klicken Sie auf **"Abmelden"**, um die Seite des PGP Universal Web Messenger zu verlassen.





Der E-Mail-Benutzer kann jederzeit auf der Seite <https://kispkey.unizh.ch> erneut auf sein sicheres Mailkonto zugreifen und Ihnen (ins Kinderspital) eine Nachricht zustellen.



Wird das Mailkonto 1 Jahr lang nicht mehr verwendet, wird es automatisch gelöscht.

2.3 Testen des PGP Universal Web Messengers

Sie können den PGP Universal Web Messenger vorgängig selber testen: Senden Sie sich selbst ein E-Mail mit der Option "**vertraulich**" auf ein privates E-Mail-Konto und richten Sie sich ein sicheres Mailkonto auf dem Kispi-Server ein.