



# eMail - aber sicher

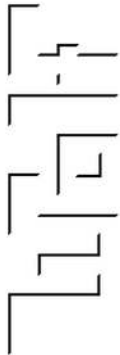
fälschungs- und abhörsichere  
Kommunikation mit S/MIME

*für Privatanwender und gewerbliche Nutzer*

## **eMail - aber sicher**

1. [Titelseite](#)
2. [1 Vorwort](#)
3. [2 Gundüberlegungen](#)
4. [3 Grundlagen und Ziele](#)
5. [4 Benötigte Mittel](#)
6. [5 Wir besorgen uns ein Zertifikat](#)
7. [6 Die Volksverschlüsselung](#)
8. [7 S/MIME verwenden](#)
9. [8 Zertifikate veröffentlichen und finden](#)
10. [9 Restrisiken](#)

# Titelseite



## eMail – aber sicher

Fälschungs- und abhörsichere Kommunikation mit S/MIME

für Privatanwender und gewerbliche Nutzer

Version 3.1

Autor:

Gunnar Wolf

gunnar@wolsland.info

© Gunnar Wolf 2019: Alle Rechte vorbehalten.

Vervielfältigung – auch auszugsweise – nur mit Zustimmung des Autors.

# 1 Vorwort

Drei Fragen vorab:

- *Sollte nicht der vorgesehene Empfänger einer eMail und kein anderer diese öffnen und lesen können?*
- *Sollte nicht jeder Empfänger einer eMail sicher sein können, dass der Inhalt unverändert ist und von der genannten Absenderadresse stammt?*
- *Wussten Sie, dass man dies auch ohne Zusatzkosten erreichen kann?*

Man muss nur mitmachen und sich ein Zertifikat besorgen.

## 1.1 Wer braucht das?

*Ich hab keine so vertraulichen Nachrichten. Meine Mails kann jeder mitlesen. Die NSA schneidet sowieso alles mit. Absolute Sicherheit gibt es nicht.*

Kennen Sie diese Aussagen auch? Sollten wir unsere Türen besser offen lassen, weil es ja sowieso keine absolute Sicherheit gibt? Warum nur verschicken manche Leute Schriftstücke in einem verschlossenen Brief?

## 1.2 Was schadet es?

Es tut niemandem weh, wenn sie Ihr Haus oder Auto abschließen. Und es schadet auch niemandem, wenn Sie die Verschlüsselung von Nachrichten an Sie für jedermann ermöglichen. Ob jemand