

PM Doc~Flow Report

DE-Mail

Unter der Begriff „DE-Mail“ läuft zur Zeit eine Initiative zur Erprobung eines sicheren Mailverkehrs. Hierzu läuft derzeit ein Pilotprojekt in Friedrichshafen.

Die DE-Mail soll einen „rechtssicheren“ elektronischen Briefverkehr ermöglichen. Dies soll dadurch sicher gestellt werden, dass alle Teilnehmer authentifiziert sind (bekannt sind) und über entsprechende Verfahren, die Unverfälschtheit und Zustellung sicher gestellt wird. Einige zentrale Punkte von DE-Mail sollen hier kurz vorgestellt werden:

- Authentifizierung: Jeder Benutzer muss sich registrieren und seine Identität erstmalig beim Diensteanbieter nachweisen. Dadurch kann später zuverlässig festgestellt werden, wer der wirkliche Absender und Empfänger einer Nachricht ist.
- Verschlüsselung: Übersandte Nachrichten werden verschlüsselt. Dadurch kann einerseits ein unberechtigtes Lesen einer Nachricht verhindert werden und andererseits wird durch spezifische Verfahren sichergestellt, dass Verfälschungen der Nachricht erkannt werden.

Durch dieses hohe Sicherheitsniveau können verschiedene wichtige Dienste angeboten werden. Dies können z.B. sein:

- „Normales“ DE-Mail stellt Vertraulichkeit sicher und schützt vor Änderung
- De-Mail-Einschreiben hat den Charakter eines Einwurfeinschreibens.
- Persönliche DE-Mail erfordert einen höheren Level der Authentifizierung von den Beteiligten

Ein De-Mail-Provider muss sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditieren, um den Nachweis zu erbringen, dass er die Anforderungen erfüllt.

Es gibt aber noch weitere Dienste für Mails und das System soll aber auch noch Zusatzfunktionen haben, wie:

- DE-Ident dient dazu, die Identität einer Person zu bestätigen. Der DE-Mail Provider verschickt mit qualifizierter Signatur einen Identitätsnachweis eines Nutzers an einen anderen Nutzer

Nr. 01/
2010

- Mit Hilfe von DE_Safe kann der Benutzer wichtige Dokumente beim Provider revisionssicher archivieren.

Es bleibt die Frage der Beurteilung von DE-Mail:

Generell ist der Ansatz zu begrüßen, ein standardisiertes Verfahren für einen sicheren Mailverkehr zu schaffen, der geeignet einen vertraulichen und rechtlich abgesicherten Informationsaustausch zu ermöglichen. Das Ziel ist hierbei, die Handhabung zu vereinfachen und zu standardisieren, so dass keine komplexe Handhabung von Zertifikaten, Verschlüsselungstechnologien etc. beim Endbenutzer notwendig ist. Dies soll letztendlich alles beim Serviceprovider erfolgen.

Im gegenwärtigen Stand der Konzeption kann man dies wohl damit erreichen. Ob sich DE-Mail allerdings durchsetzen wird, lässt sich noch nicht beurteilen – allerdings sind einige problematische Aspekte erkennbar:

- DE-Mail ist nicht kostenlos – dies ist schon eine Starthürde
- Man benötigt für DE-Mail gesonderte E-Mail-Accounts. Dies erfordert dann entweder den vollständigen Umstieg oder man hat zwei verschiedene Accounts. Im ersten Fall sind dann alle Mails gebührenpflichtig, im zweiten ist das Handling umständlich und fehleranfällig.
- Es ist noch nicht klar, wie genau die rechtliche Einstufung ist. Es wird dann darauf verwiesen, dass man DE-Mails auch mit einer qualifizierten elektronischen Signatur versehen kann, um auf der „ganz sicheren Seite“ zu sein. Dies kann man aber auch mit normalen E-Mails – dazu braucht man kein DE-Mail.

Autor:

Dr. Klaus Götzer, PM Doc~Flow