
Simulation authentifizierter Kommunikation mit gpg4Win

Aufgabe: In den Folien zu M7_09 wird der Ablauf einer authentifizierten Kommunikation mithilfe von Zertifikaten und Signaturen in einem Beispiel schematische dargestellt. Verteilen Sie die Rollen der *Bank*, der *Zertifizierungsstelle (CA)* und dem *Kunden Pingu* unter sich. Simulieren Sie den Ablauf der Kommunikation, indem Sie mit *Gpg4Win* entsprechende Nachrichten erstellen und austauschen.

Hinweis: Ein Zertifikat können Sie beispielsweise simulieren, indem Sie die Datei mit dem öffentlichen Schlüssel mit ihrem privaten Schlüssel verschlüsseln. *Gpg4Win* ermöglicht das Verschlüsseln von Dateien, indem Sie das Fenster *File Manager* öffnen. Wählen Sie über *Open*, die zu verschlüsselnde Datei aus und klicken Sie anschließend auf den Button *Encrypt*. Es wird eine verschlüsselte Kopie der Datei erstellt.

