Digital signature

This is a digital seal which creates a unique connection between a natural person and an electronic document (e.g. e-mail), which cannot be manipulated. In accordance with a certain calculation rule, a check sum (hash value) is computed from the document to be signed. The check sum is encrypted using the signatory's secret key, and then sent to recipients together with the original document. Applying the same calculation rule, they will then create another hash value from the document. Recipients also encrypt the hash value using the public key of senders which has been created by senders to start with. If both hash values are identical, they can assume that the document has arrived on their system unaltered, and that the senders are actually who they purport to be.

Copyright – All rights reserved. Lucerne School of Information Technologies