# SET Dual Signature

## by David G. Messerschmitt

Supplementary section for Understanding Networked Applications: A First Course, Morgan Kaufmann, 1999.



The dual signature is illustrated in Figure 1.. The order but not the authorization is provided to the merchant—the authorization is encrypted with the acquirer's public key, and thus the merchant can't see the plaintext—and the authorization not the order is available to the acquirer. This preserves consumer privacy—the merchant has no access to the customer's financial information, including credit card information, and the acquirer has no access to purchase information.

The dual signature nevertheless prevents customer repudiation of the *coupled* order and authorization. The message digest (MD) of the order and authorization are independently calculated by the customer. The dual signature is the encrypted (with the customer's secret key) MD of the concatenated order and authorization MD's. The dual signature is supplied to both the merchant and acquirer. The protocol arranges for the merchant to see the MD of the authorization (without seeing the authorization itself), and the acquirer sees the MD of the order (but not the order itself). The dual signature can be verified using the MD of the order or authorization—it doesn't require the order or authorization itself. Its MD does not reveal the content of the order or authorization, and thus privacy is preserved.

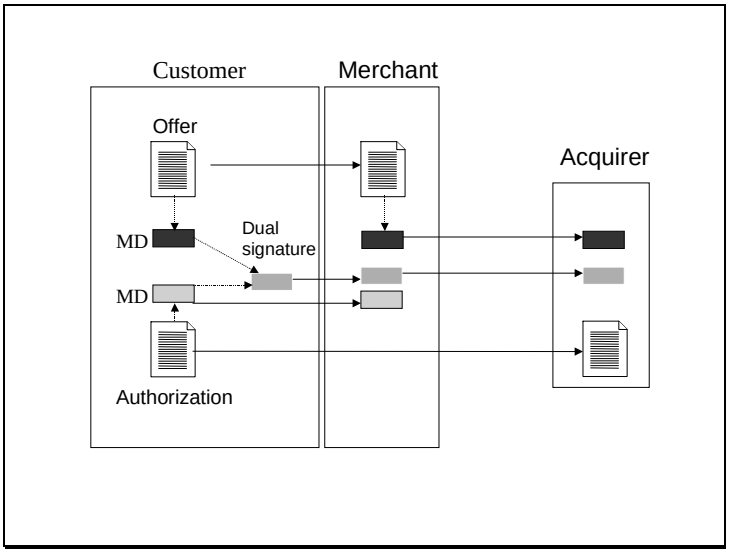


**Figure 1. The dual signature links the offer and authorization while protecting privacy.**