Some Tips...

Donald E. Eastlake 3rd
CyberCash, Inc.
dee@cybercash.com
<http://www.cybercash.com>

Customers Avoid Effort

- If your system requires lots of set up effort and there is some way to avoid your system, customers will.
- Customers don’t care about security unless they perceive a direct threat to themselves.

Merchants Care About the Sale

- Merchants want to be able to easily accept whatever type of payment the customer wants to make.
- Merchants usually don’t care about security unless they perceive a direct threat to themselves.

Signatures are Tricky

- 90%+ of cryptographic problems in a system of any complexity relate to signatures, not encryption.
- It's bad enough authenticating from A->B but when you have A->B->C, it gets really bad.
- Be sure you have had several smart people think about all the canonical form of signed content issues: time/date formats, upper/lower case letters, leading/trailing zeros/blanks, optional/default fields/values, etc. That way you will probably only have a few panics about signatures that don't verify.

Key Control is Tricky

- At least once in the development of a system of any complexity, you will try to run operationally with a test/debug key and fail.
- If your keys/certificates expire, as they should, at least one important test/demo will fail due to such expiration.
- Certificate hierarchies / key chains multiply the opportunities for problems.