Boulder Software Engineering
3021 Eleventh Street Boulder, Colorado 80304 USA
(303) 444-4541 FAX (303) 444-4541 ext. 10

19 Apr 91

NOTE → pre-5.266 !!

Jim Bidzos
RSA Data Security, Inc.
10 Twin Dolphin Drive
Redwood City, CA 94065

Dear Jim:

Well, I'm finally getting around to writing you about requesting a royalty-free license to your RSA algorithm. We talked about this a few times since your 1986 visit to Boulder, when I developed my own RSA math library in C. Both you and Ron said then and later that you would grant me a free license to make and sell products with your algorithm. I appreciate that a lot. When we last spoke, you said you would need a letter telling you what products it's for. It was unclear whether this meant highly detailed firm product plans or just general fuzzy plans. ← 1986!

There are two product areas I want to address. The most interesting is a low cost secure telephone, based on RSA, Diffie-Hellman, DES, and CELP or maybe LPC10e. This may be a standalone device, or a device that a regular phone attaches to, or an add-on device for a personal computer. If one of these works and sells, perhaps the others would also be developed.

This has been my dream product for quite a while. But to do that I need financial backing, which I have been seeking between projects on and off for a couple of years. I may be able to build such a product in some joint venture with another company. But this is still speculative at this point, because my main living is mostly gleaned from consulting on client-oriented projects. A promise of a license from you for this product would increase the chances of getting backing for such a venture. You can help me crack the chicken-and-egg cycle. How about a letter of intent? *

The other product area is more realizable, and that would be a set of software products to do RSA/DES encryption, RSA/MD4 signatures, and some other related functions for personal computers. This would be somewhat analogous to your Mailsafe or Comsafe products. I guess it would sort of compete with these products. I suspect these products are not the backbone of your company's cashflow, anyway. I just think they would be fun for me to do. I probably would not be developing that jointly with another company, but I may sell it through another company's marketing channels. $ #

As a "true believer" in RSA technology since 1977, I will continue in my consulting to try to steer my clients toward your technology. I've been working with such a client for a while now. It's hard to find projects in this area, and like any other substantial project it takes a long time in the R&D cycle to bring a project to fruition for a client who is willing to use RSA. When I get my client there, they will have to pay you for your algorithm. They can better afford to pay your licensing fees than I can. I hope I can scratch your back this way as much as possible. I hope you can scratch mine too.

Please give me a call if you need any more information. Or even if you don't. It's been a while since we spoke, and it would be nice to hear from you again just to see how you're getting along.

Thanks,

Philip R. Zimmermann

Philip Zimmermann

cc: Ron Rivest

* The PSP doc lie about RSA having "promised" a license. Does he have such a letter? NO! In fact I sent a letter saying no.