Exhibit B

PATENT INVALIDITY CONTENTIONS FOR U.S. Patent No. 6,704,870

U.S. Patent No. 6,704,870
Title: DIGITAL SIGNATURE ON A SMART CARD
Filed: August 29, 2001
Issued: March 9, 2004

Identification and Date of Relevant Prior Art (P.R. 3-3(a)):

Publication: Dr. Alfred J. Menezes, Dr. Mingua Qu and Dr. Scott Vanstone, "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," dated October 30, 1994, published at least as early as November 1, 1994.

Japanese Laid-Open Patent Application PH6-43809
Title: DIGITAL SIGNATURE SYSTEMS BASED ON ELLIPTIC CURVE AND ITS SIGNER DEVICE AND VERIFIER DEVICE
Published: February 18, 1994.

Publication: "Responses to NIST's Proposal," Communications of the ACM, July 1992.

Publication: Alfred Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers (1993).

Publication: "Digital Signature Standard (DSS)," Federal Information Standards Publication 186, published May 19, 1994.

U.S. Patent No. 5,231,668
Title: DIGITAL SIGNATURE ALGORITHM
Filed: July 26, 1991
Published: July 27, 1993.

Basis of Invalidity (P.R. 3-3(b)):

Anticipation:
Claims 1 and 2 are invalid under 35 U.S.C. § 102(b) as anticipated by each of (a) IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, dated (the "IEEE P1363 Oct. 1994 Draft"), (b) Japanese Laid-Open Patent Application PH6-43809 ("JP '809 Application"), (c) Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal"), and (d) Elliptic Curve Public Key Cryptosystems," by Alfred Menezes (the "Menezes book"). Each of these references either expressly or inherently discloses each of the method steps of claim 1 and 2.

Claims 3 and 18 are invalid under 35 U.S.C. § 102(b) as anticipated by each of (a) the IEEE P1363 Oct. 1994 Draft, (b) Responses to NIST's Proposal, and (c) the Menezes book. Each of these references either expressly or inherently discloses each of the method steps of claims 3 and 18.

Claim 21 is invalid under 35 U.S.C. § 102(b) as anticipated by each of the IEEE P1363 Oct. 1994 Draft and the JP '809 Application. Each of these references anticipates claim 21 because it either expressly or inherently discloses each of the method steps of claim 21.

Claim 22 is invalid under 35 U.S.C. § 102(b) as anticipated by the IEEE P1363 Oct. 1994 Draft. This reference anticipates claim 22 because it either expressly or inherently discloses each of the method steps of claim 22.

Obviousness:
Claims 1, 2, 3, 18, 21 and 22 are invalid under 35 U.S.C. § 103 as obvious over each of (a) the IEEE P1363 Oct. 1994 Draft, (b) the JP '809 Application, (c) Responses to NIST's Proposal, and (d) the Menezes book, either alone, in view of FIPS-DSS or the '668 Patent, or in any combination of any of the foregoing.

Motivation to Combine Items of Prior Art:
It would have been obvious to a person of ordinary skill in the art at the time of the alleged invention to combine any of the IEEE P1363 Oct. 1994 Draft, the JP '809 Application, Responses to NIST's Proposal and the Menezes book with either of FIPS-DSS or the '668 Patent. FIPS-DSS and the '668 Patent both disclose the Digital Signature Algorithm ("DSA") from the Digital Signature Standard ("DSS") proposed by the U.S. Government Agency National Institute for Standards and Technology ("NIST"). Each of the IEEE P1363 Oct. 1994 Draft, the JP '809 Application, NIST's Proposal and the Menezes book reference use this algorithm as a basis for their elliptic curve-based system. That is, each discloses an elliptic curve analog of DSA. Accordingly, a person of ordinary skill in the art would have been motivated to combine any of the IEEE P1363 Oct. 1994 Draft, the JP '809 Application, NIST's Proposal and the Menezes book with either FIPS-DSS or the '668 Patent.

Invalidity Claim Chart (P.R. 3-3(c)):

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").

	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of:	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.1, p. 6; 6.1.2 p. 7.
	2) JP '809 Application at [0001], p. 4; at [Claim 1], p .3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12; at p. 13.
	5) FIPS-DSS at p. 5.
	6) '668 Patent, at col. 4:34-35.[1]
i) selecting as a session key an integer k	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:19-28.
and computing representation of a corresponding point kP;	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:29-30; at col. 5:37-42.
ii) deriving from said	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.

[1] This document uses the notation x:a-b to refer to Column x lines a-b in a patent.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
representation a first signature component, r, independent of said message, m;	**2) JP '809 Application** at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:.29-36.
iii) combining said first signature component, r, with a private key, a, a value derived from said message, m, and said session key, k, to obtain a second [10] signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r,s, are made public; and	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, pp.7- 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12**.**
	5) FIPS-DSS at p. 5.
	6) '668 Patent, at col. 6:4-10**.**
iv) utilizing said signature components r,s, in the signature of the message, m.	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
	6) '668 Patent at col. 6:13-16.
2. A method according to claim 1 wherein said value derived from said message, m, is obtained by applying a hash function to said message.	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:63-6:10.
3. A method according to claim 2 wherein said second signature component, s, is of the form s=k.sup.-1 {h(m)+ar} mod q,	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p.2.
	6) '668 Patent at col. 6:4-10.
where q is a divisor of the order,	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.1.1, p. 6.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
e, of said elliptic curve	**2) JP '809 Application** at [Claim 1], p.3.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:.48-49.
and h(m) is said value derived by applying a hash function to said message.	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, pp. 7-8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6)'668 Patent at col. 5:63-6:10.
18. A method according to claim 1 wherein said second signature component s has a value corresponding to $[k^{1}\{h(m)+ar\} \bmod q]$ $\underline{k^{-1}\{h(m)+ar\} \bmod q}$.	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 6:4-10.
21. A method of generating a digital signature r, s, of a message m using an elliptic curve cryptosystem employing an elliptic curve of order e, said method comprising the steps of:	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.1, p. 6; at 6.1.2, p. 7.
	2) JP '809 Application at [0001], p. 4; at [Claim 1], p.3.; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at 13.
	5) FIPS-DSS at p. 5.
	6) '668 Patent, at col. 4:34-35.
i) selecting an integer k and determining a corresponding point kP where P is point on the curve;	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:19-28; at col. 5:29-30; col. 5:37-42.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
ii) selecting a coordinate (x) of the point kP;	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:29-30; at col. 5:37-42.
iii) reducing the coordinate mod q where q is a known divisor of e, to obtain a first component r; and	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.1, p. 6; at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	5) FIPS-DSS at p. 5.
	6) '668 Patent at col. 5:29-37; at col. 5:48-49.
iv) combining said first component, r, with a long-term private key a and [10] said integer k to obtain a second signature component s, such that extraction of either said long term private key a or said integer k is inhibited even when	**1) IEEE P1363 Oct. 1994 Draft** at 6.1.2, p. 8.
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.

U.S. Patent No. 6,704,870	**1) "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, October 30, 1994 (the "IEEE P1363 Oct. 1994 Draft").**
	2) Japanese Laid-Open Patent Application PH6-43809 (citations to English translation) ("JP '809 Application").
	3) "Responses to NIST's Proposal," Communications of the ACM, July 1992 ("Responses to NIST's Proposal").
	4) "Elliptic Curve Public Key Cryptosystems," by Alfred Menezes, published 1993 ("Menezes book").
	5) "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186, published May 19, 1994 ("FIPS-DSS").
	6) U.S. Patent No. 5,231,668 to Kravitz, issued on July 27, 1993 ("'668 Patent").
said signature r,s, are made public.	**5) FIPS-DSS** at p. 5.
	6) '668 Patent at col. 6:4-10.
22. A method according to claim 21 wherein said second signature component s has the form [$s=k^1\{h(m)+ar\} \bmod q$] $\underline{s=k^{-1}\{h(m)+ar\} \bmod q}$, where h(m) is a hash of the message m.	**1)** "Use the private key d to compute $s := k^{-1}(m + rd) \bmod n$." **IEEE P1363 Oct. 1994 Draft at 6.1.2, p. 8.**
	2) JP '809 Application at [Claim 1], p.3; at [0007], p. 6.
	3) Responses to NIST's Proposal at p. 51.
	4) Menezes book at p. 12.
	5) FIPS-DSS at p. 5.
	6)'668 Patent at col. 5:63-6: 10.

Basis of Invalidity (P.R. 3-3(d)):
Claim 21 and 22 are invalid under 35 U.S.C. § 112, ¶¶ 1 and 2 because the term "long- term" is vague and indefinite, and lacks written description support.

Claims 3, 18 and 22 are invalid under 35 U.S.C. § 112, ¶ 1 as lacking written description with respect to the phrases "said second signature component, s, is of the form $s=k^{-1}\{h(m) + ar\} \bmod q$," "said second signature component s has a value corresponding to $k^{-1}\{h(m) + ar\}$", and "said second signature component s has the form $s=k^{-1}\{h(m)+ar\} \bmod q$," respectively.

Claims 1, 3, 18, 21 and 22 are invalid under 35 U.S.C. § 112, ¶¶ 1 and 2 as lacking enablement, and as vague and indefinite with respect to the phrases “selecting as a session key an integer k,” and “selecting an integer k.”