



Improving 2D Bar Code Security with ECC

Topics

- Company Background
- Certicom Products
- Certicom Bar Code Security
- Demo

ECC and RSA Recommend Key Sizes

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	Elliptic Curve Asymmetric Algorithms	RSA/DSA/DH Asymmetric Algorithms	Expected Lifetime Expiry
56 bits	DES				Expired
80 bits	3DES (2 key)	SHA-1	163 bits	1024 bits	2010
112 bits	3DES (3 key)	SHA-224	233 bits	2048 bits	2030
128 bits	AES-128	SHA-256	256 bits	3072 bits	2031+
192 bits	AES-192	SHA-384	384 bits	7680 bits	2031+
256 bits	AES-256	SHA-512	512 bits	15360 bits	2031+

Why ECC?

- **ECC - next generation public key cryptography**
- **Digital signatures provide non-repudiation**
 - Non-repudiation prevents an entity from denying previous commitments or actions
 - Allows off-network authentication
- **International standards based**
 - IEEE 1363a-2004, FIPS and or NESSIE
 - ECDSA digital signature for authentication
 - ECPVS digital signature for authentication with encryption to protect privacy
- **Performance**
 - ECC 163 bit curve has equivalent security level to 1024 bit RSA
 - ECC digital signature is $\sim \frac{1}{4}$ the size of RSA
 - The difference increases with key strength
 - ECC signing speed is many times faster



Adding Signatures to 2D Bar Codes

	Bar Code Data (characters)	Digital Signature (characters)	Total Data Written (characters)
RSA – 1024 bits	183	172	355
ECDSA – 163 bits	183	56	239
ECPVS – 163 bits	183	56	239
RSA – 2048 bits	183	344	527
ECDSA – 233 bits	183	80	263
ECPVS – 233 bits	183	76	259

- PEM encode signatures
- ECPVS offers smallest signature size as well as ability to hide portions of the message

163 ECC Versus 1024 RSA Using 183 Characters – PDF417

The top row shows three screenshots of the certicom boarding pass generation interface. Each screenshot displays the same passenger information (Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527) and flight details (Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135). The main difference is the signature type and the resulting barcode data.

- Left Screenshot:** Signature Type: No Signature. Barcode Data: SGRIFPHS/MICHAEL KQKBR AC 1 7347 YZYZZ #W YLAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1. Barcode Size: 183 characters.
- Middle Screenshot:** Signature Type: ECCDSA 163 bit. Barcode Data: SGRIFPHS/MICHAEL KQKBR AC 1 7347 YZYZZ #W YLAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1. Barcode Size: 239 characters.
- Right Screenshot:** Signature Type: ECPVS 163 bit. Barcode Data: SGRIFPHS/MICHAEL KQKBR AC 1 7347 YZYZZ #W YLAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1. Barcode Size: 239 characters. A red arrow points to the 'Hidden Data' field, which contains the frequent flyer number 0937553527.

Each screenshot also shows the boarding pass details: GRIFFITHS MICHAEL, Economy Class / Classe Economique, ETKT0142152650617, Frequent Flyer / Voyeur assidû *3527 A, Flight/Avion AC 0480 13DEC, From/De TORONTO-T1, Destination MONTREAL, Boarding Time/Heure d'embarquement 05:45, Gate/Porte 135, Seat/Place 27F, and a QR code.

Frequent flyer number is now encrypted using ECPVS

163 ECC Versus 1024 RSA Using 500 Characters – PDF147

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHTS/MICHAEL KOKBJR AC 1 7347 YYZY2 J#W YULAC 0400 3 47Y5 Z7F 0018A JPC101421526506 17 AC0937553527P E*1

Signature: Signature Type: No Signature, Barcode Format: PDF417, Increase data to 500 Bytes: , Barcode Size: 500 characters

Hidden Data: [] Update Barcode

Boarding Pass

GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617


Frequent Flyer / Voyeur assidue
*3527 A

Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL

Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F

Departure Time/heure de départ: 06:30
Air Time use/A usage interne: 0088 WC20070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHTS/MICHAEL KOKBJR AC 1 7347 YYZY2 J#W YULAC 0400 3 47Y5 Z7F 0018A JPC101421526506 17 AC0937553527P E*1

Signature: Signature: A#H837M#Nz0z3Y#Wz9#0R#b#m#A5y7 ++s#OpL#6i#C#N#C#W#s#R, Signature Type: ECC5A 163 bit, Barcode Format: PDF417, Increase data to 500 Bytes: , Barcode Size: 556 characters

Hidden Data: [] Update Barcode

Boarding Pass

GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617


Frequent Flyer / Voyeur assidue
*3527 A

Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL

Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F

Departure Time/heure de départ: 06:30
Air Time use/A usage interne: 0088 WC20070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHTS/MICHAEL KOKBJR AC 1 7347 YYZY2 J#W YULAC 0400 3 47Y5 Z7F 0018A JPC101421526506 17 AC*****P E*1

Signature: Signature: ++s#OpL#6i#C#N#C#W#s#R, Signature Type: ECCP5 163 bit, Barcode Format: PDF417, Increase data to 500 Bytes: , Barcode Size: 556 characters

Hidden Data: 0937553527 Update Barcode

Boarding Pass

GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617


Frequent Flyer / Voyeur assidue
*3527 A

Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL

Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F

Departure Time/heure de départ: 06:30
Air Time use/A usage interne: 0088 WC20070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHTS/MICHAEL KOKBJR AC 1 7347 YYZY2 J#W YULAC 0400 3 47Y5 Z7F 0018A JPC101421526506 17 AC0937553527P E*1

Signature: Signature: E#agP#9#nd#H#0#v#v#B#R#0#i#2#d#v#P #L#0#2#0#R#F#4#S#2#v#s#9#P#Q#z#H#6#L#T# #T#T#v#Q#v#B#T#0#V#L#W#K#S#R#R#0# #L#F#B#S#S#Z#W#S#Z#W#K#S#R#0#v#Q#z#J#M #P#F#B#d#W#U#S#4#3#0#n#A#F#L#U#S#H#N#J#A #0#2#z#A#Q#0#=#, Signature Type: RSA 1024 bit, Barcode Format: PDF417, Increase data to 500 Bytes: , Barcode Size: 672 characters

Hidden Data: [] Update Barcode

Boarding Pass

GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617

Frequent Flyer / Voyeur assidue
*3527 A

Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL

Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F

Departure Time/heure de départ: 06:30
Air Time use/A usage interne: 0088 WC20070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit



233 ECC Versus 2048 RSA Using 500 Characters - PDF417

board

Passenger: Last Name: GRIFFITHS First Name: MICHAEL Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617 Flight Number: 0400 From: TORONTO-T1 To: MONTREAL
Seat: 27F Boarding Time: 05:45 Gate: 135

Barcode Data: Signature: Signature Type: No Signature
Barcode Format: PDF417
 Increase data to 500 Bytes
Barcode Size: 500 characters

Hidden Data: [] Update Barcode

Boarding Pass


GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617 Frequent Flyer / Voyeur assidue *3527 A

Flight/Avion From/De Destination
AC 0480 13DEC TORONTO-T1 MONTREAL

Boarding Time/heure d'embarquement 05:45 Gate/Porte 135 Seat/Place 27F

Departure Time/heure de départ 06:30
Air Time use/A usage interne 0088 M320070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS First Name: MICHAEL Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617 Flight Number: 0400 From: TORONTO-T1 To: MONTREAL
Seat: 27F Boarding Time: 05:45 Gate: 135

Barcode Data: Signature: Signature Type: ECC5A 233 bit
Barcode Format: PDF417
 Increase data to 500 Bytes
Barcode Size: 500 characters

Hidden Data: [] Update Barcode

Boarding Pass


GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617 Frequent Flyer / Voyeur assidue *3527 A

Flight/Avion From/De Destination
AC 0480 13DEC TORONTO-T1 MONTREAL

Boarding Time/heure d'embarquement 05:45 Gate/Porte 135 Seat/Place 27F

Departure Time/heure de départ 06:30
Air Time use/A usage interne 0088 M320070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS First Name: MICHAEL Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617 Flight Number: 0400 From: TORONTO-T1 To: MONTREAL
Seat: 27F Boarding Time: 05:45 Gate: 135

Barcode Data: Signature: Signature Type: ECCP5 233 bit
Barcode Format: PDF417
 Increase data to 500 Bytes
Barcode Size: 576 characters

Hidden Data: 0937553527 Update Barcode

Boarding Pass


GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617 Frequent Flyer / Voyeur assidue *3527 A

Flight/Avion From/De Destination
AC 0480 13DEC TORONTO-T1 MONTREAL

Boarding Time/heure d'embarquement 05:45 Gate/Porte 135 Seat/Place 27F

Departure Time/heure de départ 06:30
Air Time use/A usage interne 0088 M320070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

board

Passenger: Last Name: GRIFFITHS First Name: MICHAEL Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617 Flight Number: 0400 From: TORONTO-T1 To: MONTREAL
Seat: 27F Boarding Time: 05:45 Gate: 135

Barcode Data: Signature: Signature Type: RSA 2048 bit
Barcode Format: PDF417
 Increase data to 500 Bytes
Barcode Size: 844 characters

Hidden Data: [] Update Barcode

Boarding Pass

GRIFFITHS MICHAEL
ECONOMY CLASS / CLASSE ECONOMIQUE
ETKT0142152650617 Frequent Flyer / Voyeur assidue *3527 A

Flight/Avion From/De Destination
AC 0480 13DEC TORONTO-T1 MONTREAL

Boarding Time/heure d'embarquement 05:45 Gate/Porte 135 Seat/Place 27F

Departure Time/heure de départ 06:30
Air Time use/A usage interne 0088 M320070

Boarding Pass | Carete d'accès à bord



certicom securing innovation

Exit

163 ECC Versus 1024 RSA Using 183 Characters – Data Matrix

The first three screenshots show the boarding pass generation process for Michael Griffiths on flight AC 0480 from Toronto to Montreal. The interface includes fields for passenger information, flight details, and barcode options. The 'Signature Type' dropdown is set to 'No Signature', 'ECC5A 163 bit', and 'ECPS 163 bit' respectively. The 'Barcode Size' is 183 characters for all three. The boarding pass preview shows the passenger name, flight details, and a QR code.

The fourth screenshot shows the boarding pass generation process for Michael Griffiths on flight AC 0480 from Toronto to Montreal. The 'Signature Type' dropdown is set to 'RSA 1024 bit'. The 'Barcode Size' is 355 characters. The boarding pass preview shows the passenger name, flight details, and a QR code.



233 ECC Versus 2048 RSA Using 183 Characters – Data Matrix

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHS/MICHAEL KOKBR AC 1 7347 YYZY Z JW YULAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1

Signature Type: No Signature, Barcode Format: Data Matrix, Barcode Size: 183 characters

Hidden Data: [Empty]

Boarding Pass: GRIFFITHS MICHAEL, Frequent Flyer/Avoyeur assid: *3527 A, Flight/Av: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL, Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F, Departure Time/heure de depart: 06:30, Airline use/A usage interne: 0088 MC20070

Boarding Pass | Carete d'accès à bord

certicom securing innovation

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHS/MICHAEL KOKBR AC 1 7347 YYZY Z JW YULAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1

Signature: 018121hewh8g13k7wYCO0+DGO+Pz 3H94+uZTfGkqgT23V1S2238RfB1 y3AA3kZ7ahA3Q==

Signature Type: ECC5A 233 bit, Barcode Format: Data Matrix, Barcode Size: 263 characters

Hidden Data: [Empty]

Boarding Pass: GRIFFITHS MICHAEL, Frequent Flyer/Avoyeur assid: *3527 A, Flight/Av: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL, Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F, Departure Time/heure de depart: 06:30, Airline use/A usage interne: 0088 MC20070

Boarding Pass | Carete d'accès à bord

certicom securing innovation

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHS/MICHAEL KOKBR AC 1 7347 YYZY Z JW YULAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC*****P E*1

Signature: 8f6v33bc328EfhgrpW0j+vgheN t0h6rMADfweyFL30hWdKniqggo uRQ3um8Pw==

Signature Type: ECPSV 233 bit, Barcode Format: Data Matrix, Barcode Size: 259 characters

Hidden Data: 0937553527

Boarding Pass: GRIFFITHS MICHAEL, Frequent Flyer/Avoyeur assid: *3527 A, Flight/Av: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL, Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F, Departure Time/heure de depart: 06:30, Airline use/A usage interne: 0088 MC20070

Boarding Pass | Carete d'accès à bord

certicom securing innovation

board

Passenger: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527

Flight Information: Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135

Barcode Data: SGRIFPHS/MICHAEL KOKBR AC 1 7347 YYZY Z JW YULAC 0400 3 47Y5 ZPF 0018A JPC101421526506 17 AC0937553527P E*1

Signature: f1spenq2fYyVkdQ2ghcQ8Rm3w1p0t 1h9g0cWRP0225fpa>Lc0h7j9c 4h0c0s4u4nk0203hA90THWcM EdChofv6w6g6wkcsczwldng.D6e02Q YScn93xm4L3m51sbw9ECLal0n26 3p33hMvFvFvVqBw6h033Scap9E3 Gf0R2VgJFwCDNfMBA0o0k0Hf5gk

Signature Type: RSA 2048 bit, Barcode Format: Data Matrix, Barcode Size: 527 characters

Hidden Data: [Empty]

Boarding Pass: GRIFFITHS MICHAEL, Frequent Flyer/Avoyeur assid: *3527 A, Flight/Av: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL, Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135, Seat/Place: 27F, Departure Time/heure de depart: 06:30, Airline use/A usage interne: 0088 MC20070

Boarding Pass | Carete d'accès à bord

certicom securing innovation



163 ECC Versus 1024 RSA Using 500 Characters - Data Matrix

The first three screenshots show the boarding pass interface with different signature configurations:

- Left Screenshot:** Signature Type: No Signature. Barcode Size: 500 characters.
- Middle Screenshot:** Signature Type: ECC5A 163 bit. Barcode Size: 556 characters.
- Right Screenshot:** Signature Type: ECPS 163 bit. Barcode Size: 556 characters.

Each screenshot displays the following information:

- Passenger:** GRIFITHS, MICHAEL, Frequent Flyer: 0937553527
- Flight Information:** Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135
- Barcode Data:** SGRIFITHS/MICHAEL KOKBJR AC 1 7347 YYZYZ JW YULAC 0400 3 47YS ZPF 0018A JPC101421526506 17 AC0937553527P E*1
- Hidden Data:** 0937553527
- Boarding Pass:**
 - GRIFITHS MICHAEL
 - ECONOMY CLASS / CLASSE ECONOMIQUE: ETKT0142152650617
 - Frequent Flyer/Numéro assidue: *3527 A
 - Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL
 - Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135
 - Departure Time/heure de départ: 06:30
 - Airline use/A usage interne: 0088 MCB0070
 - Boarding Pass | Carete d'accès à bord

The fourth screenshot shows the boarding pass interface with the following configuration:

- Signature Type:** RSA 1024 bit. Barcode Size: 672 characters.

The boarding pass information is identical to the previous screenshots:

- Passenger:** GRIFITHS, MICHAEL, Frequent Flyer: 0937553527
- Flight Information:** Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135
- Barcode Data:** SGRIFITHS/MICHAEL KOKBJR AC 1 7347 YYZYZ JW YULAC 0400 3 47YS ZPF 0018A JPC101421526506 17 AC0937553527P E*1
- Hidden Data:** 0937553527
- Boarding Pass:**
 - GRIFITHS MICHAEL
 - ECONOMY CLASS / CLASSE ECONOMIQUE: ETKT0142152650617
 - Frequent Flyer/Numéro assidue: *3527 A
 - Flight/Avion: AC 0480 13DEC, From/De: TORONTO-T1, Destination: MONTREAL
 - Boarding Time/heure d'embarquement: 05:45, Gate/Porte: 135
 - Departure Time/heure de départ: 06:30
 - Airline use/A usage interne: 0088 MCB0070
 - Boarding Pass | Carete d'accès à bord



233 ECC Versus 2048 RSA Using 500 Characters - Data Matrix

The image displays three side-by-side screenshots of a boarding pass generation interface. Each window shows the same passenger information: Last Name: GRIFFITHS, First Name: MICHAEL, Frequent Flyer: 0937553527, Ticket Number: 0142152650617, Flight Number: 0400, From: TORONTO-T1, To: MONTREAL, Seat: 27F, Boarding Time: 05:45, Gate: 135. The interface includes fields for Barcode Data, Signature, Signature Type, Barcode Format, and Barcode Size. The first window shows 'No Signature' and 'Data Matrix' format. The second window shows 'ECDSA 233 bit' and 'Data Matrix' format. The third window shows 'ECDSA 2048 bit' and 'Data Matrix' format. The boarding pass information is displayed below, including the name GRIFFITHS MICHAEL, frequent flyer number *3527 A, flight details AC 0480 13DEC TORONTO-T1 MONTREAL, boarding time 05:45, gate 135, and a QR code. The certicom logo is visible at the bottom of each window.

Data Matrix limit of 780
RSA 2048 with 500
characters exceeds the limit

ECC Usage in the Airline Industry

ACARS Evolution

- **ACARS**
 - The Basic System
- **Secure ACARS (S-ACARS)**
 - The interim Proposal
 - Proof-of-Concept
 - Used Certicom Security Builder Modules
- **Protected ACARS (P-ACARS)**
 - The next Proposal
 - Will use the Production grade ECC Certificates

Secure ACARS

- **Provides a secure channel of communication between aircrafts and ground stations**
 - authentication, integrity, and encryption
- **ECC preferred to RSA due to limited resources**
 - power, CPU, storage
- **Certicom designed a custom version of System Security Object (SSO) component with Security Builder (SB) Crypto-C and SB PKI-C**
 - sect163r1 and sect233r1 elliptic curves
 - ECDSA-with-SHA1/SHA-256:
 - ECDH

Protected ACARS

- ARINC, Honeywell, Rockwell, and the Air Force Research Lab (AFRL) are developing a PKI solution to implement Protected ACARS
 - Elliptical Curve Cryptography
 - ARINC Project Paper 823
 - Datalink Security Part 1 – ACARS Message Security (AMS)
 - Datalink Security Part 2 – Key Management
 - sect233r1 Elliptic curve based PKI
 - 128-bit based random shared secret key Key Management Infrastructure (KMI)

Certicom ECC Conference 2007

