certicom
securing innovation

Improving 2D Bar Code Security with ECC

아이콤정보시스템
TEL:02)861-1175 , FAX:02)861-1176

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 ~¼ the size of RSA
      - The difference increases with key strength
    - ECC signing speed is many times faster

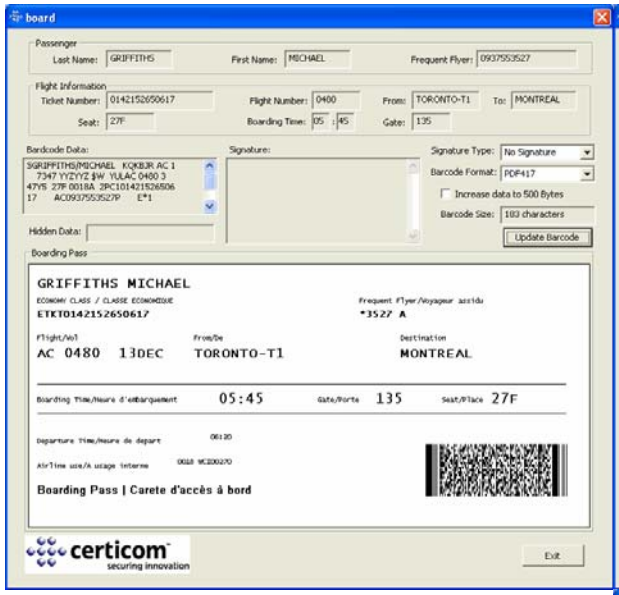
iCom IComis certicom

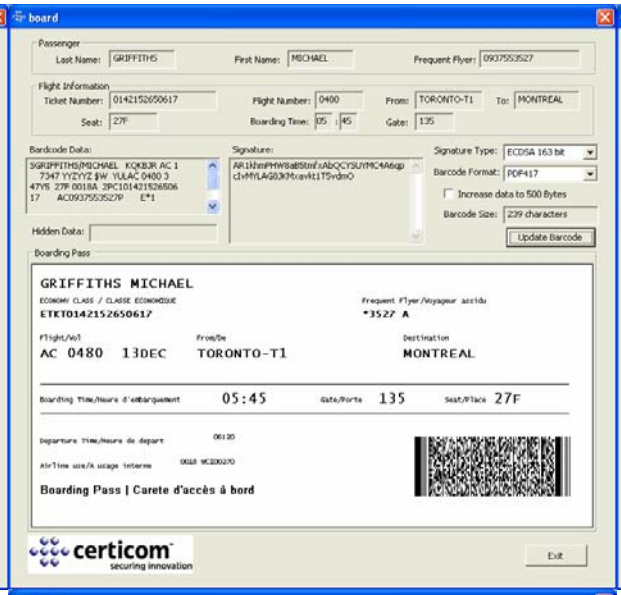
Adding Signatures to 2D Bar Codes

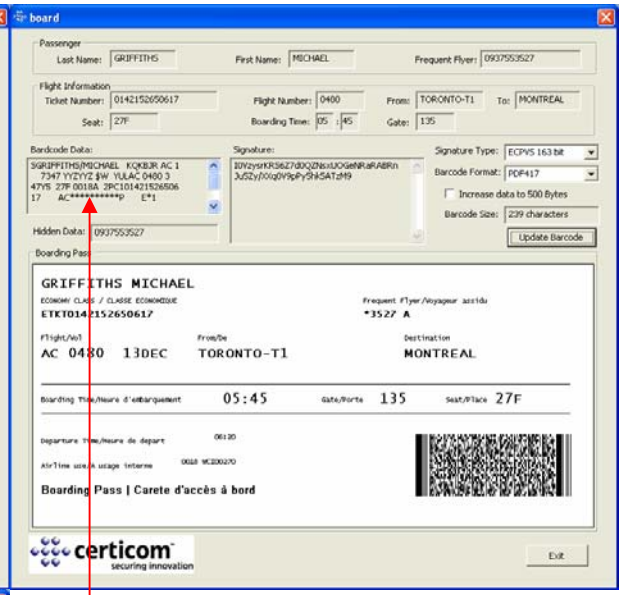
	Bar Code Data (characters)	Digital Signature (characters)	Total Data Written (characters)
RSA – 1024 bits	183	172	355
ECDSA – 163 bits	183	56	239
ECPVS – 163 bits	183	56	239
RSA – 2048 bits	183	344	527
ECDSA – 233 bits	183	80	263
ECPVS – 233 bits	183	76	259

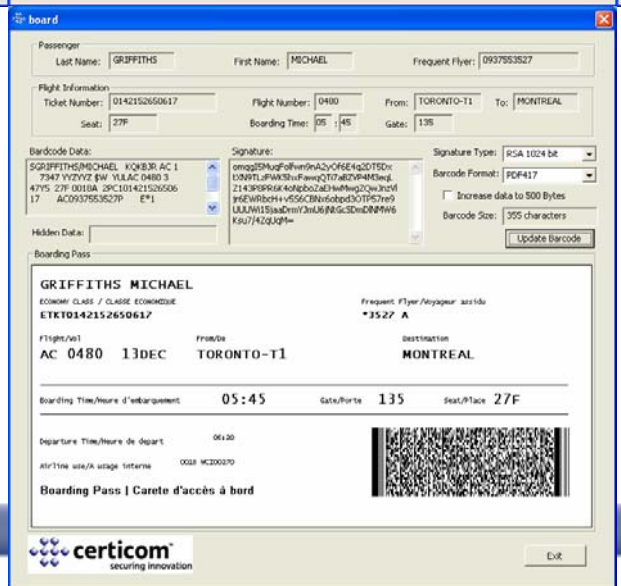
- PEM encode signatures
- ECPVS offers smallest signature size as well as ability to hide portions of the message

163 ECC Versus 1024 RSA Using 183 Characters – PDF417





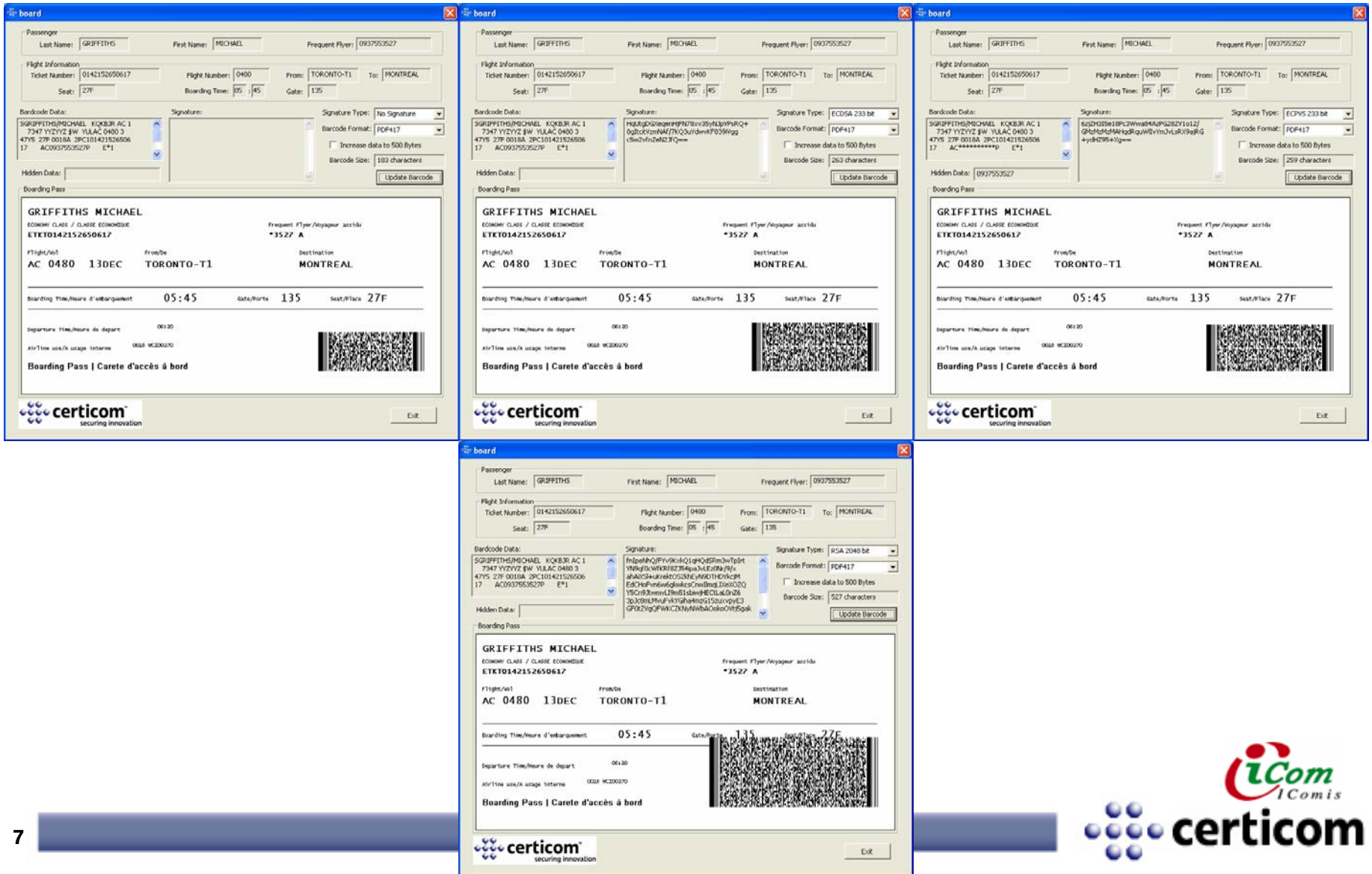




Frequent flyer number is now encrypted using ECPVS

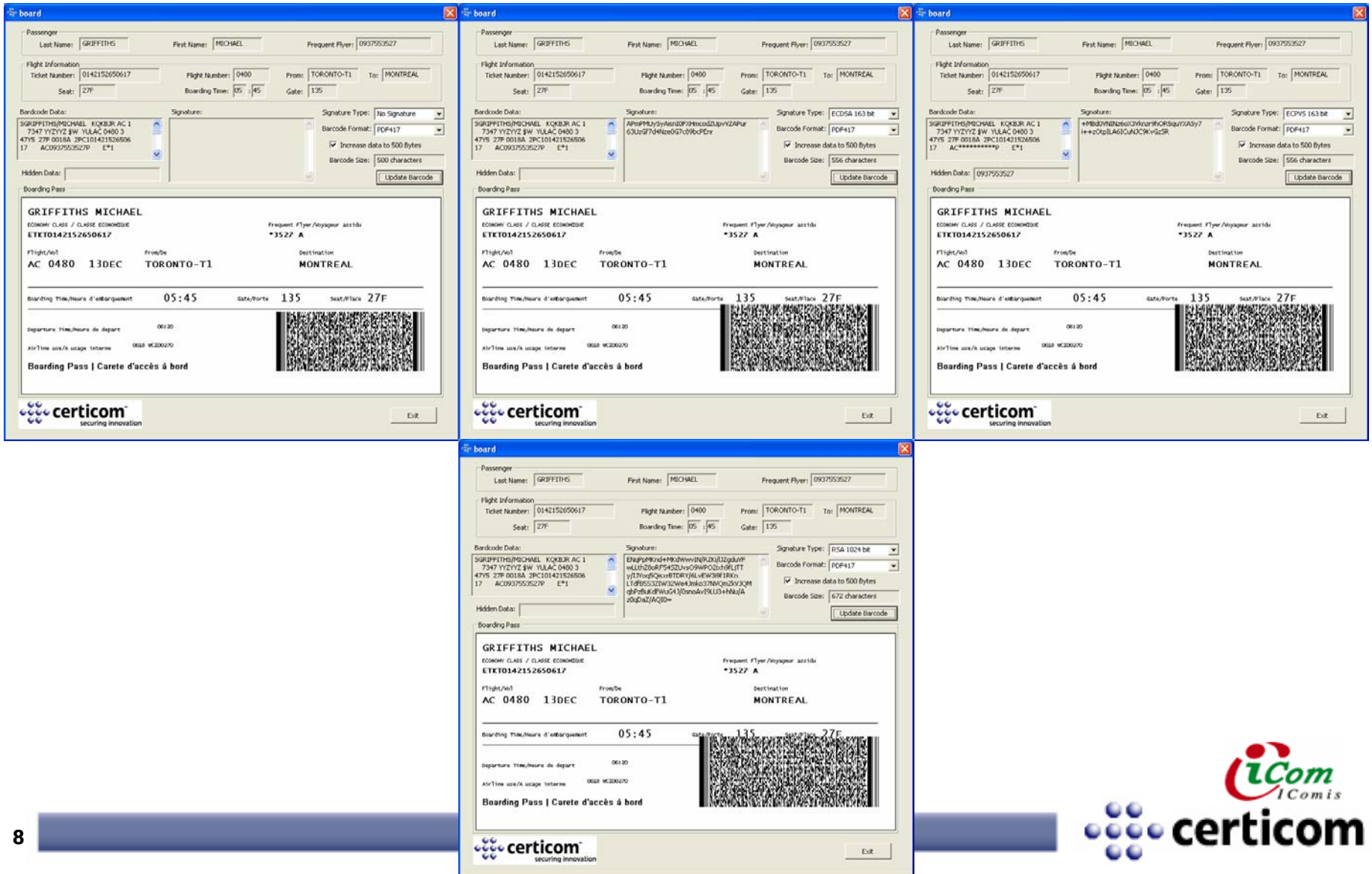
iCom IComis certicom

233 ECC Versus 2048 RSA Using 183 Characters – PDF417



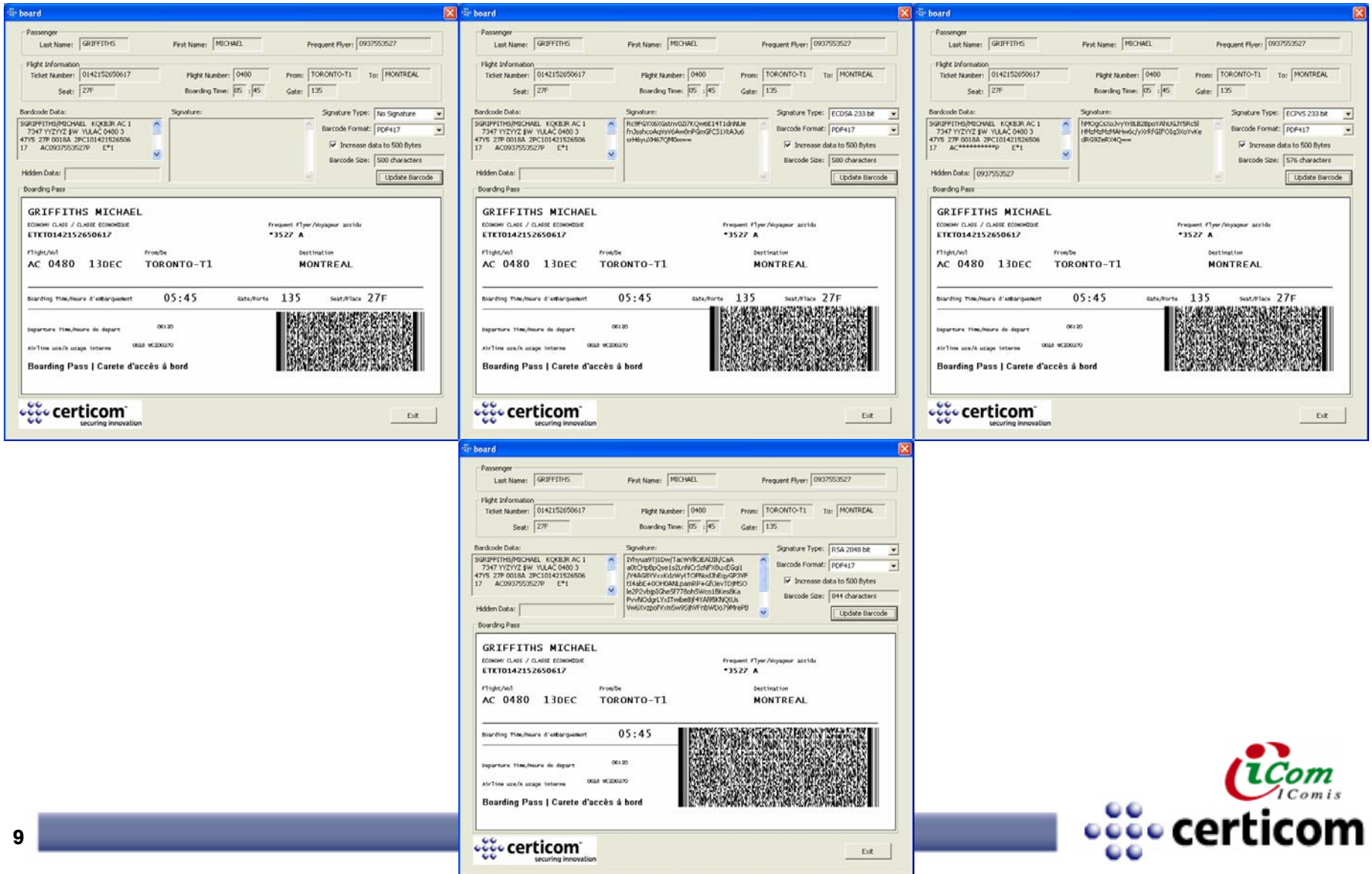
iCom
iComis
certicom

163 ECC Versus 1024 RSA Using 500 Characters – PDF147



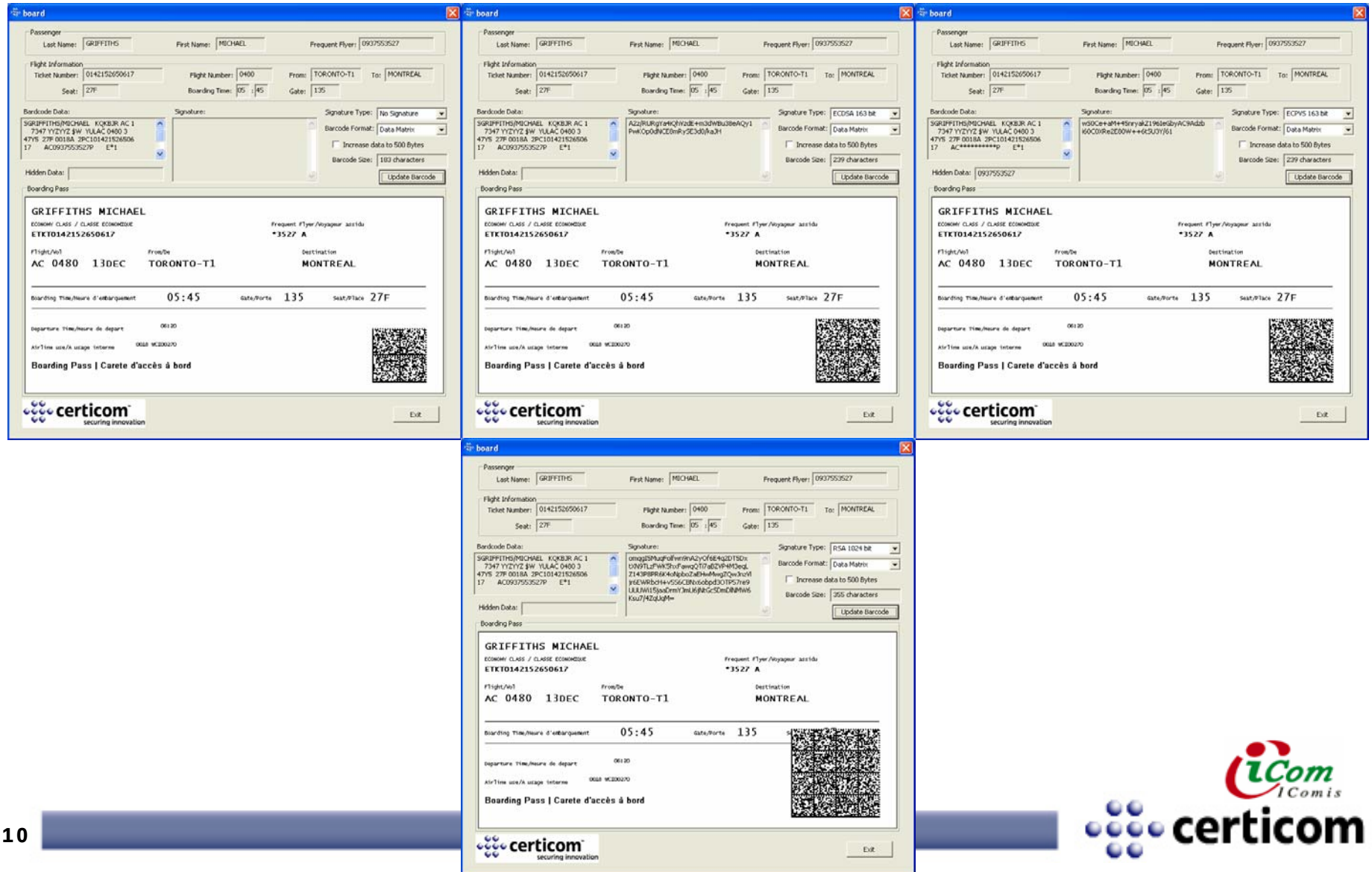
iCom
Comis
certicom

233 ECC Versus 2048 RSA Using 500 Characters - PDF417



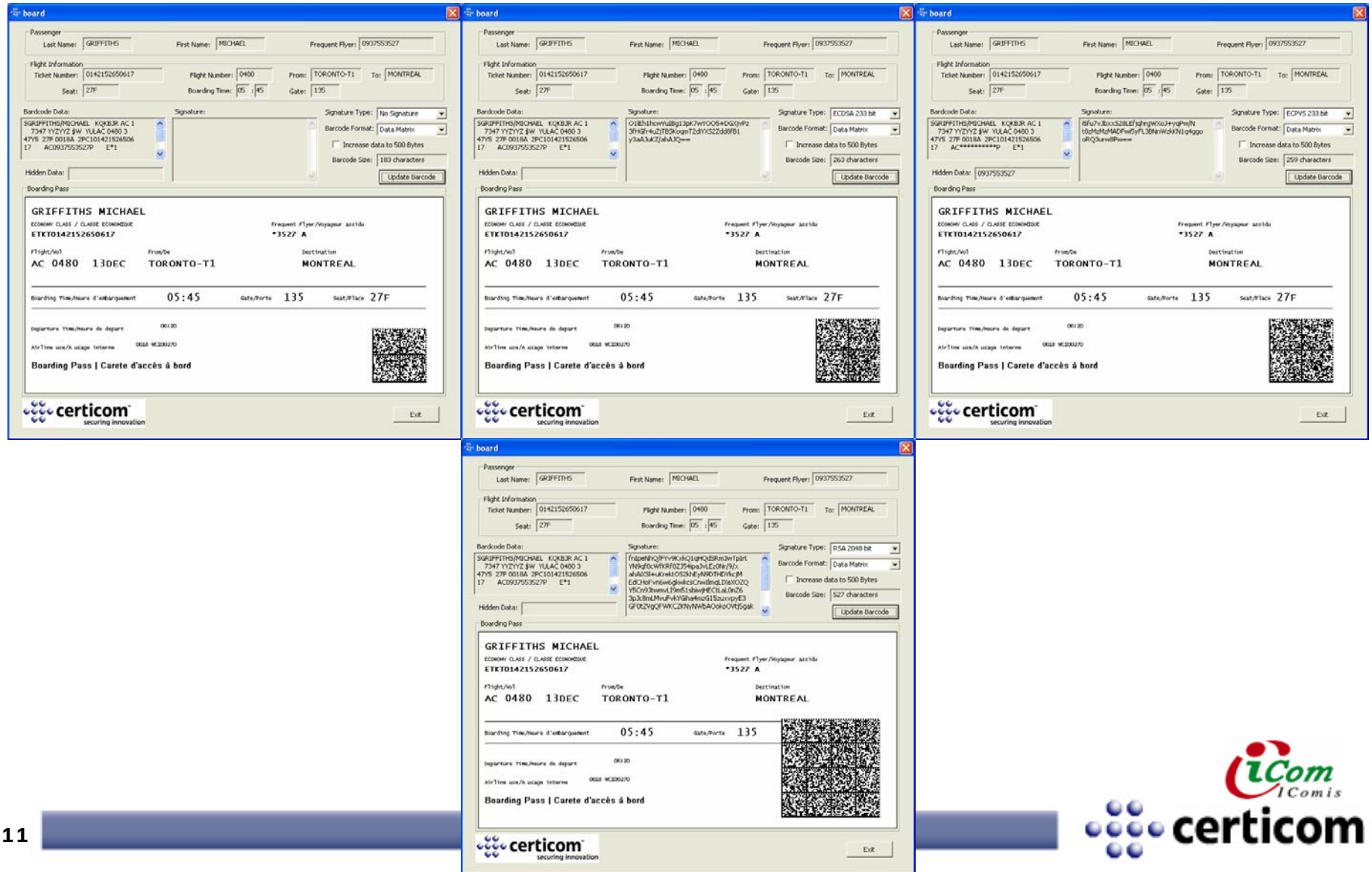
iCom
iComis
certicom

163 ECC Versus 1024 RSA Using 183 Characters – Data Matrix



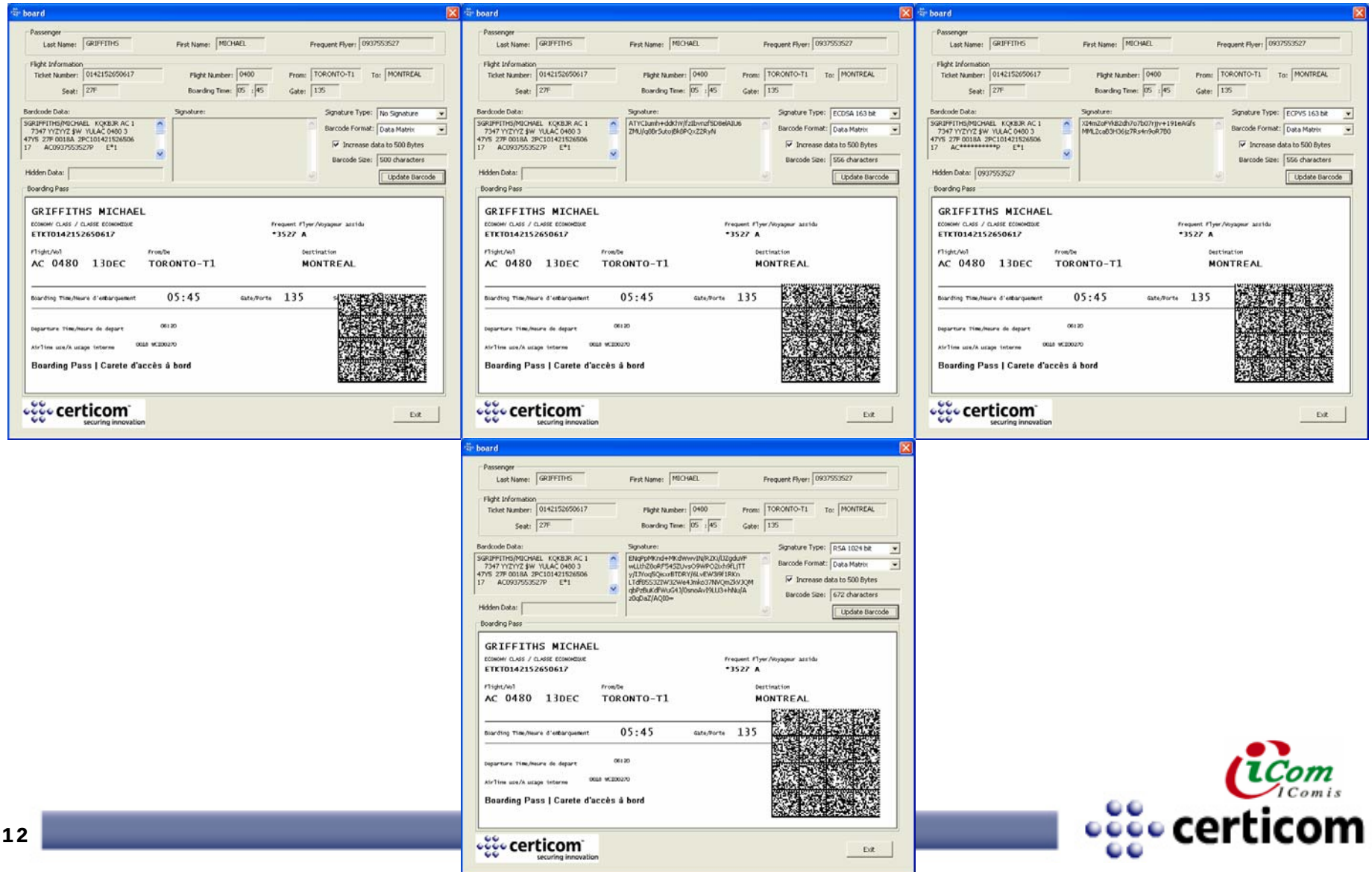
iCom
Comis
certicom

233 ECC Versus 2048 RSA Using 183 Characters – Data Matrix



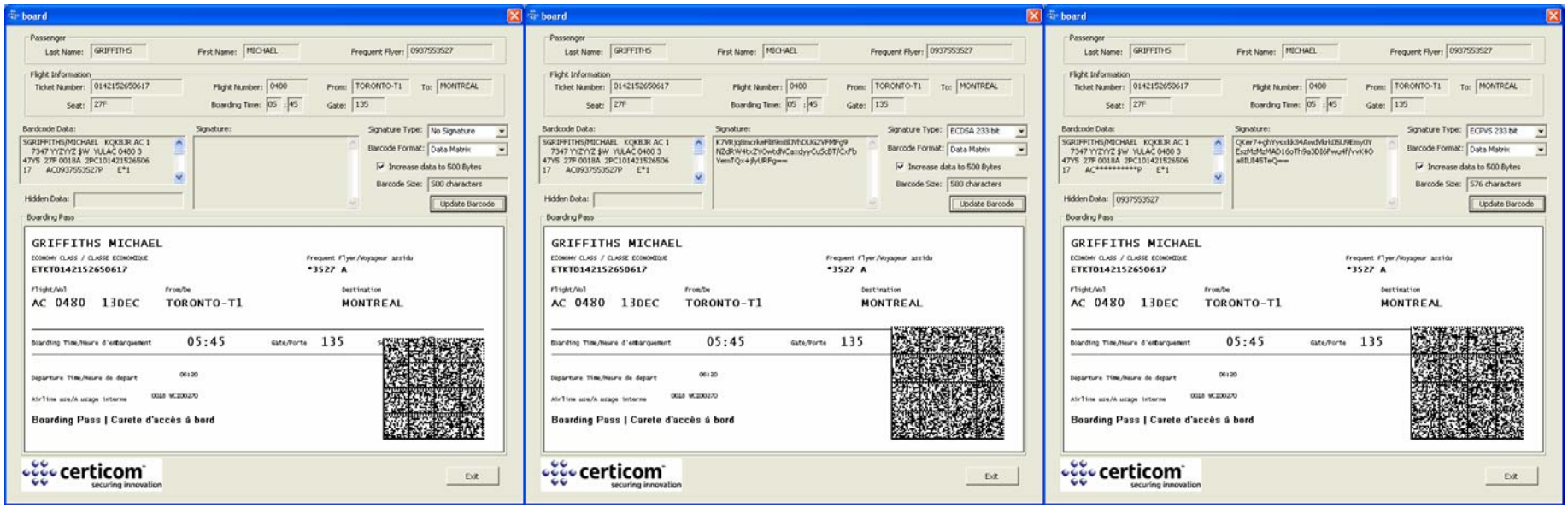
iCom
I Comis
certicom

163 ECC Versus 1024 RSA Using 500 Characters - Data Matrix



iCom
I Comis
certicom

233 ECC Versus 2048 RSA Using 500 Characters - Data Matrix



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

iCom
I Comis
certicom

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

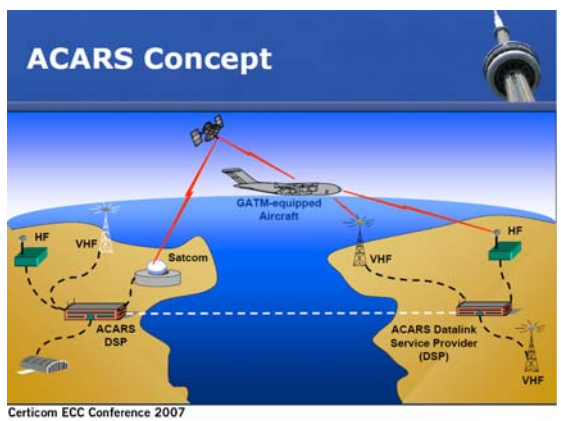
Secure ACARS

- **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



certicom