



certicom

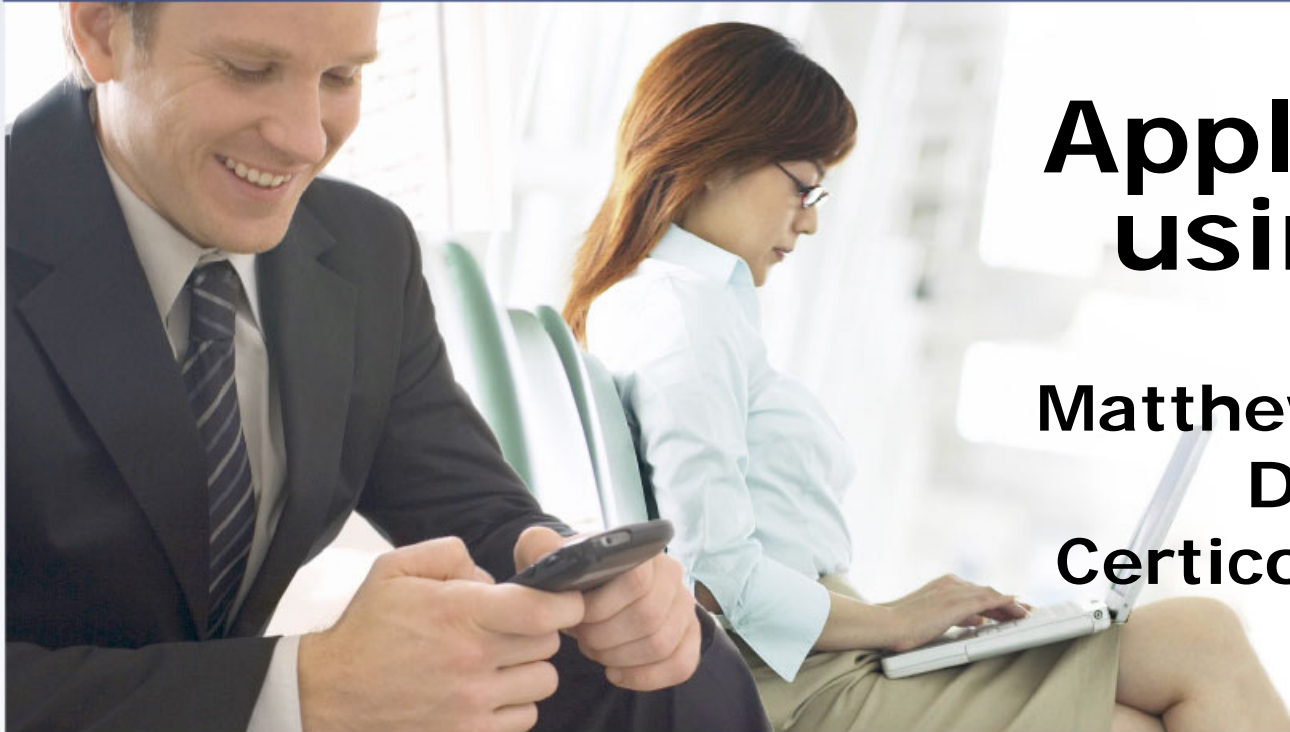
securing innovation

**protect your content,
applications and devices**

with government-approved security



certicom
securing innovation



Applications using ECC

Matthew Campagna
Director
Certicom Research

Agenda

- About Certicom
- Pitney Bowes PC Smart Meter
- BlackBerry Smartcard Reader
- New techniques for financial applications and bandwidth constrained environments
 - Elliptic Curve Pintsov-Vanstone
 - Elliptic Curve Qu-Vanstone

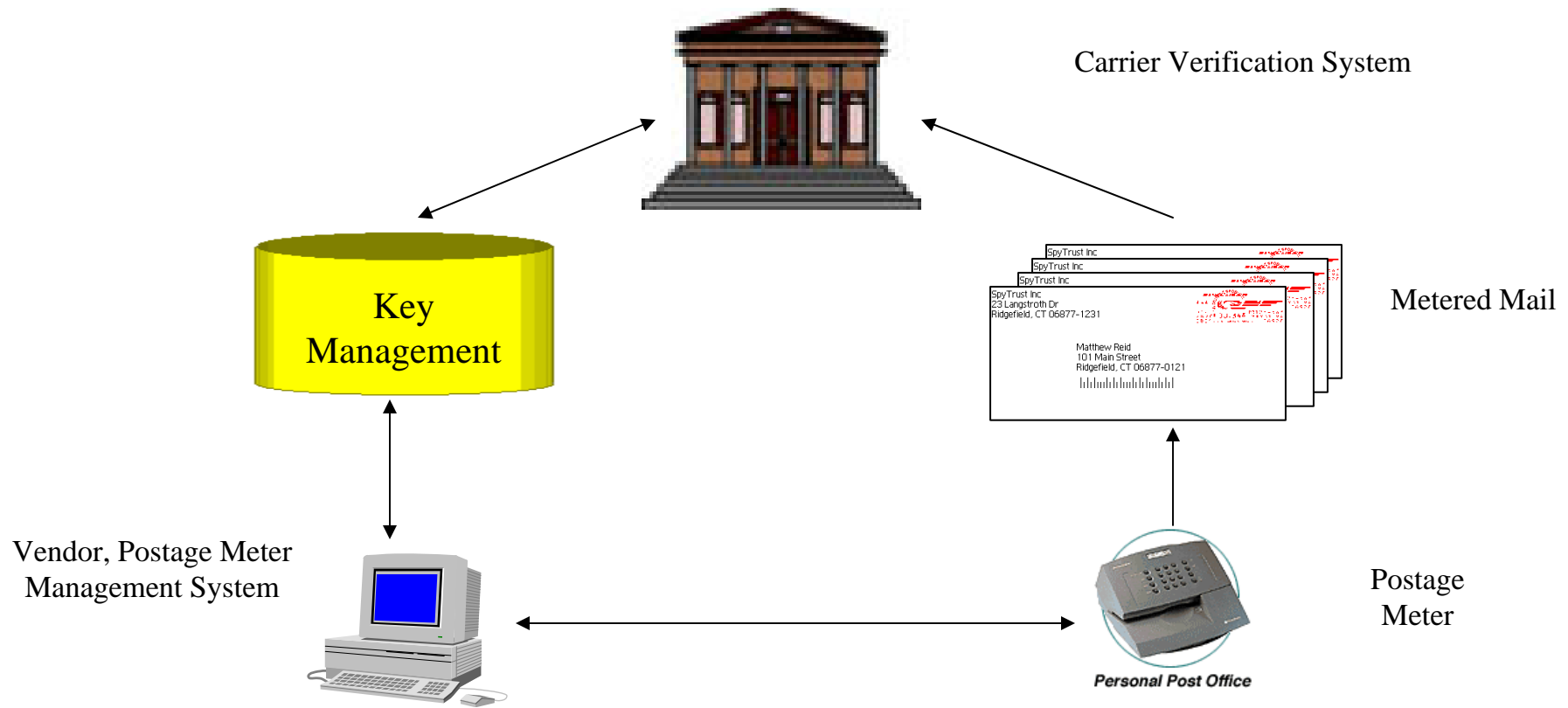
About Certicom

- Founded in 1985 by Dr. Scott Vanstone, University of Waterloo
- 120+ Employees
- Offices in Toronto, San Francisco, Washington DC, Ottawa & London (UK)
 - New sales presence in Asia Pacific and Israel
- License software products, patents & services to OEMs who embed security
- Recently acquired by BlackBerry maker Research In Motion

PC Smart Meter

- 1997 Pitney Bowes completed a smartcard based postage meter
- Designed to be used with a PC with spurious connectivity to the Internet
- The meter consists of a trusted FIPS 140, Level 3 module
- Implemented IEEE P1363 Standard (working draft) of ECDSA

Postage meter system



PC Smart Meter

- Meter has an ECDSA key pair and maintains a currency amount in a postal security device within the FIPS boundary
- Meter dispenses postage and signs a structure
 - Meter ID, Amt of postage, amount in meter
 - Renders data in 2D-datamatix
- Postal sorting facility
 - Reads data, looks up public key certificate
 - Verifies signature
 - Records information for other auditing

BlackBerry Smart Card Reader

- The BlackBerry Smart Card Reader is a small, lightweight, wearable smart card reader that enables controlled access to BlackBerry smartphones and PCs.



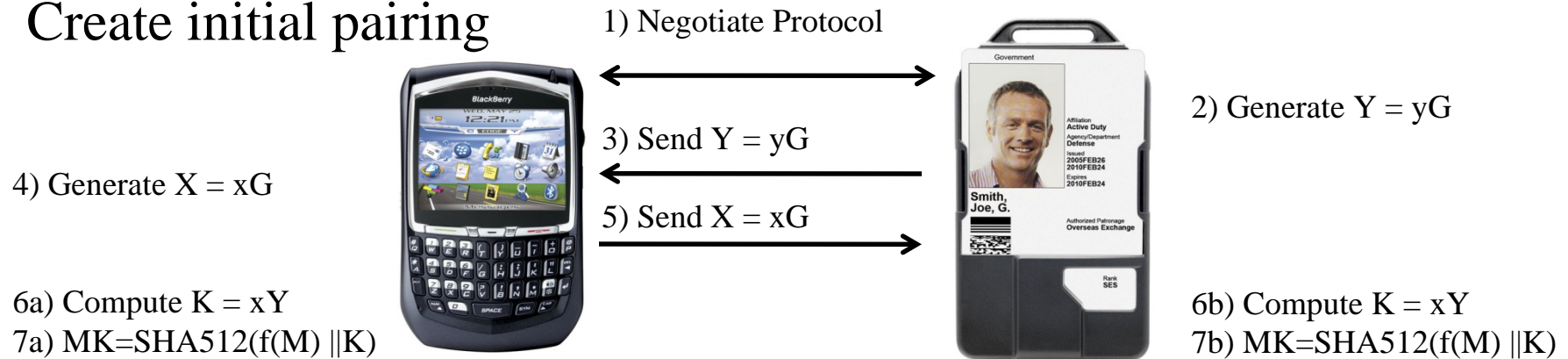
BlackBerry Smart Card Reader

Can use with BlackBerry smartphone and PC simultaneously
Individual proximity access control
Create a secure channel protected by AES256-CBC, SHA512--
HMAC

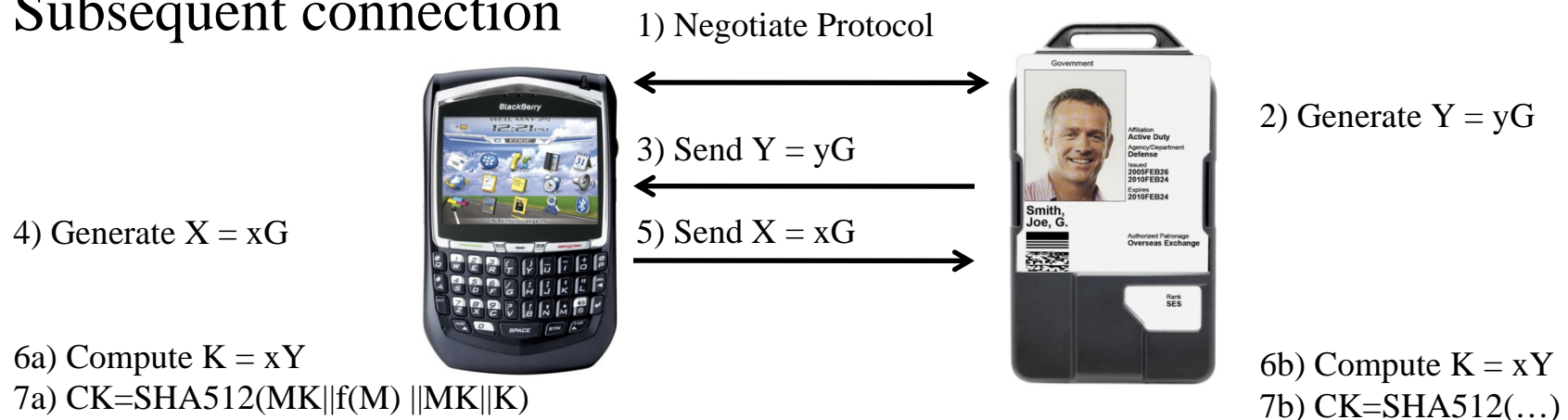


BlackBerry Smart Card Reader

Create initial pairing



Subsequent connection



BlackBerry Smart Card Reader

- Security
 - Bluetooth only used for communication, not for security
 - AES-256 encryption on all Bluetooth communication
 - Uses a FIPS 140-2 validated encryption module
- Hardware-based security model
- JVM Authentication
- Approved for use throughout U.S. Department of Defense
 - Details on BlackBerry Secure Technical Implementation Guide on DISA website

BlackBerry Smart Card Reader

Crypto component	Specification
Curves for ECDH	571-bit Koblitz Curve (EC571K1) 521-bit Random Curve (EC521R1)* 283-bit Koblitz Curve (EC283K1) 256-bit Random Curve (EC256R1) 160-bit Random Curve (EC160R1)
Encryption	AES256* AES128
Hashing	SHA512* SHA256 SHA1
Modes	CBC
MAC	HMAC

New Techniques (ECPVS)

Elliptic Curve Pintsov Vanstone Signature Scheme (ECPVS)

Input: message $m||r$, where r satisfies a redundancy requirement, and private key d_A

Output: signed message $m, (c, s)$
generate ephemeral key pair (d, Q)
construct $k = KDF(Q)$
encrypt $c = E_k(r)$.
hash $e = H(c||m)$
calculate $s = ed_A + d \pmod{n}$
return $m, (c, s)$

Benefit: Reduction in signature size by 1/2.

Standardized: ANS X9.92, IEEE P1363a, SECG SEC 3

Deployed: Postal applications, SMS applications

New Techniques (ECQV)

Elliptic Curve Qu-Vanstone Certificates (ECQV)

Implicit certificates of the form

$\{ID, QID\}$ an identifier and a compressed point
compared to

$\{ID, QID, (s, r)\}$, an explicitly signed certificate

Benefit: Reduction of cryptographic component in
certificate by 1/3.

Standardized: SECG SEC 4.

Deployed: ZigBee, Postal Applications, SMS
applications

Bit Strength to Primitive Sizes(in bytes)

Cryptographic Strength	ECDSA signature size	ECPVS signature size	RSA signature size	ECDSA certificate size	ECQV certificate size	RSA certificate size
64 bits	28	14	64	42+	14+	128+
80 bits	40	20	128	60+	20+	256+
112 bits	56	28	256	84+	28+	512+
128 bits *	64	32	384	96+	32+	768+
192 bits	96	48	960	144+	48+	1920+
256 bits *	128	64	1920	192+	64+	3840+

References

- **ANS X9.62**, American National Standards for Financial Services, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ANS X9.92**, American National Standards for Financial Services, Public Key Cryptography for the Financial Services Industry, Digital Signature Algorithm Giving Partial Message Recovery
- Blackberry Smart Card Reader Security, Version 1.5 Technical Overview
- **FIPS 140**, Security Requirements for Cryptographic Modules
- **FIPS 186-2**, Digital Signature Standard (DSS)
- **IEEE 1363-2000**, Standard Specifications for Public Key Cryptography.
- **IEEE P1363a**, Standard Specifications for Public Key Cryptography: Additional Techniques (Draft).
- **SEC 3**, Standards for Efficient Cryptography, Elliptic Curve Signatures Giving Partial Message Recovery, <http://www.secg.org>
- **SEC 4**, Standards for Efficient Cryptography, Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) <http://www.secg.org>

Contact Certicom

Matthew Campagna
Director, Certicom Research
Certicom Corp.
mcampagna@certicom.com



**protect your content,
applications and devices**

with government-approved security