

# New Crypto-Kid on the Block...!

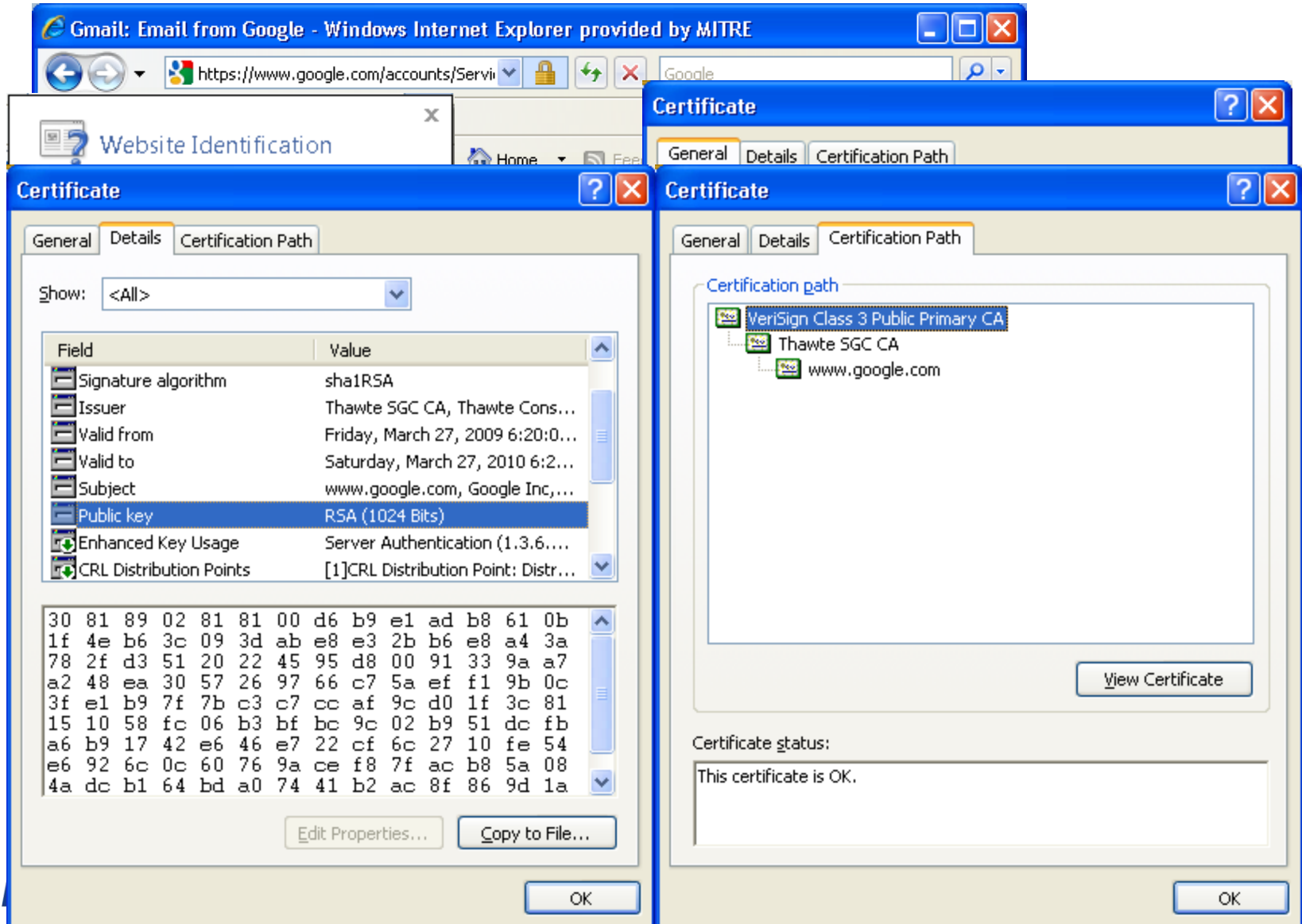
## Elliptic Curve Cryptography (ECC)

Sunil J. Trivedi

The MITRE Corporation

# Google Login

<https://www.google.com/accounts/ServiceLogin?....>



Gmail: Email from Google - Windows Internet Explorer provided by MITRE

Website Identification

Certificate

Certificate

Certificate

General Details Certification Path

General Details Certification Path

General Details Certification Path

Show: <All>

Field	Value
Signature algorithm	sha1RSA
Issuer	Thawte SGC CA, Thawte Cons...
Valid from	Friday, March 27, 2009 6:20:0...
Valid to	Saturday, March 27, 2010 6:2...
Subject	www.google.com, Google Inc,...
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication (1.3.6...
CRL Distribution Points	[1]CRL Distribution Point: Distr...

```
30 81 89 02 81 81 00 d6 b9 e1 ad b8 61 0b
1f 4e b6 3c 09 3d ab e8 e3 2b b6 e8 a4 3a
78 2f d3 51 20 22 45 95 d8 00 91 33 9a a7
a2 48 ea 30 57 26 97 66 c7 5a ef f1 9b 0c
3f e1 b9 7f 7b c3 c7 cc af 9c d0 1f 3c 81
15 10 58 fc 06 b3 bf bc 9c 02 b9 51 dc fb
a6 b9 17 42 e6 46 e7 22 cf 6c 27 10 fe 54
e6 92 6c 0c 60 76 9a ce f8 7f ac b8 5a 08
4a dc b1 64 bd a0 74 41 b2 ac 8f 86 9d 1a
```

View Certificate

Certificate status:  
This certificate is OK.

OK

OK

# Current Public Key Cryptography

- **Everywhere, almost all the time**
  - Hardware, Software, Firmware (or some combination)
  - By almost all business entities
    - Government, Financial Institutes, Web Merchants, ....
- **Typical components are:**
  - RSA public keys (mostly 1024, may be 2048)
  - SHA-1 for digest
  - RSA signature and verification
  - DES or 3-DES for encryption using symmetric key
- **Based on (one-way) server authentication**
  - SSL/TLS protocols
- **Mutual authentication**

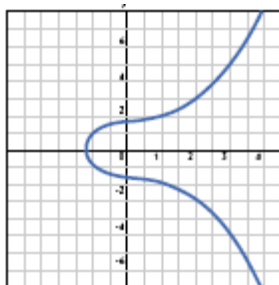
# Cryptography Evaluation in USA

- **Computer Security Resources Center (CSRC) of National Institute of Standards and Technology (NIST)**
- **The Cryptographic Algorithm Validation Program (CAVP)**
- **Federal Information Processing Standards (FIPS) 140-2**
  - **Describes requirements for Cryptographic Modules**
  - **A Mandatory Standard for all US Federal agencies using cryptographic based security systems**
- **Cryptographic Module Validation Program (CMVP)**
  - **Validates according to FIPS 140-2 and other standards**
- **Common Criteria (CC) evaluates crypto implemented products against**
  - **A Protection Profile (PP) or a Security Target (ST)**

# Elliptic Curve Cryptography (ECC)

- ECC was discovered in 1985 by Dr. Neal Koblitz and Dr. Victor Miller. Math background at:
  - [http://www.secg.org/secg\\_docs.htm](http://www.secg.org/secg_docs.htm)
  - [http://csrc.nist.gov/publications/fips/fips186-3/fips\\_186-3.pdf](http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf)
- An elliptic curve is a gently looping line of various forms as defined above. It is a two dimensional  $x, y$  Cartesian Coordinate System equation:

$$y^2 = x^3 + ax + b$$



- Certicom developed several ECC based security solutions (over 300 patents)

# Finite Field and Elliptic Curve Groups Analogues

	Finite Field Groups	Elliptic Curve Groups
Setting	Integers modulo $p$	Curve $E$ over integers modulo $p$
Basic operation	Multiplication mod $p$	Addition of points
Main operation	Exponentiation	Scalar multiplication
Accomplished by	Repeated squares and multiplies	Repeated doubles and adds
Base element	Generator integer $g$	Generator point $G$
Private key	Integer $x$	Integer $x$
Public key	$y = g^x \pmod{p}$	$W = xG$ (point on $E$ )

- Any algorithm using Exponentiation Modulo  $p$  can be translated into one using Elliptic Curves Modulo  $p$ 
  - Not true for Integer Factorization Cryptography (IFC), RSA

# ECC Algorithms

- The Elliptic Curve Digital Signature Algorithm (ECDSA)
- The Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm
- The ECC with Menezes-Qu-Vanstone (ECMQV) key exchange algorithm
- Additional ECC algorithms
  - ECSPEKE for wireless applications
  - ECPVS for digital mailing systems

# What is Changing?

- **2005: NSA published Suite B algorithms**
  - **Next Slide**
- **ECDSA Validation List (130+ Validations)**
  - <http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsaval.html>
- **Validated FIPS 140-1/2 Crypto Modules implementing ECC algorithms**
  - <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm>
- **ECC is ready for prime time**

# Suite B Algorithms

[http://www.nsa.gov/ia/programs/suiteb\\_cryptography/index.shtml](http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml)

Encryption	Advanced Encryption Standard (AES) - FIPS 197 (with keys sizes of 128 and 256 bits) <a href="http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf">http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf</a>
Digital Signature	Elliptic Curve Digital Signature Algorithm - FIPS 186-2/3 (using the curves with 256 and 384-bit prime moduli) <a href="http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf">http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf</a>
Key Exchange:	Elliptic Curve Diffie-Hellman NIST Special Publication 800-56A (using the curves with 256 and 384-bit prime moduli) <a href="http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf">http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf</a>
Hashing:	Secure Hash Algorithm - FIPS 180-2 (using SHA-256 and SHA-384) <a href="http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf">http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf</a>

# What Else is Changing?

- **Increased demand for bandwidth**
  - We spend more time on Internet than on TV
- **Proliferation of wireless applications**
  - Smart-phones, wireless networks
  - Need for smaller payload (r u ter?)
- **Organized underground market**
  - Email and credit card lists swapped and sold
- **More processing power available**
  - Less computational difficulty in factoring the RSA modulus
- **Sophisticated hackers**
  - Need for efficient cryptography

# NIST Recommended Key Sizes

<b>Security Strength (bits)</b> (Symm & Hash Algorithms)	<b>RSA and DH Key sizes (bits)</b>	<b>ECC Key Sizes (bits)</b>	<b>Safe Until</b>
<b>80</b> (3DES 2 way & SHA1)	<b>1024</b>	<b>160</b>	<b>Present – 2010</b>
<b>112</b> (3DES 3 way & SHA 224)	<b>2048</b>	<b>224</b>	<b>Present – 2030</b>
<b>128</b> (AES-128 & SHA-256)	<b>3072</b>	<b>256</b>	<b>Present – 2031 and beyond</b>
<b>192</b> (AES-192, & SHA-384)	<b>7680</b>	<b>384</b>	<b>Present – 2031 and beyond</b>
<b>256</b> (AES-256 & SHA-512)	<b>15360</b>	<b>521</b>	<b>Present – 2031 and beyond</b>

**NIST SP 800-57, Recommendation for Key Management**  
[http://www.nsa.gov/business/programs/elliptic\\_curve.shtml](http://www.nsa.gov/business/programs/elliptic_curve.shtml)

# ECC Advantages / Disadvantages

## ■ Advantages

- Smaller keys
- ECC unique scalar arithmetic
- Faster cryptographic operations
- Less heat and power consumption
- Smaller real estate (Personal Identity Verification (PIV) cards)
- Lower memory and bandwidth demands (Wireless)

## ■ Disadvantages

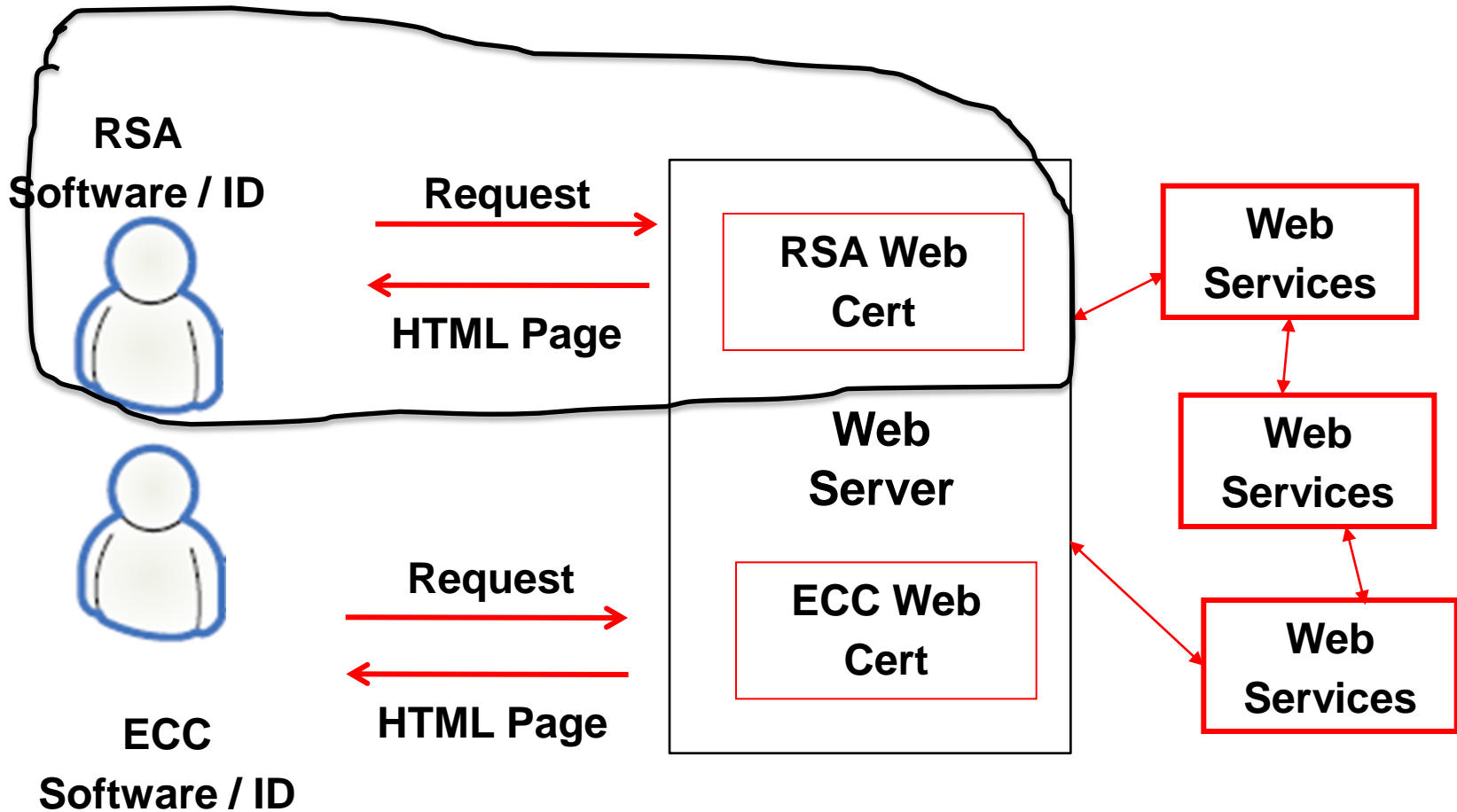
- Licenses
- Not as many developers

# ECC Applications

- ECDSA and Check 21 Bank Applications
- ECPVS and Digital Postage Marks (Pitney Bowes)
- ECDH in TLS/SSL ECC/TLS Interoperability Forum at <http://dev.experimentalstuff.com:8082/>
- ECMQV for WiFi and WiMax applications
- ARINC PP 823 specified use of ECC for encrypting text-based messages
  - P-ACARS (Protected Aircraft Communications and Reporting System)
- EU Passport

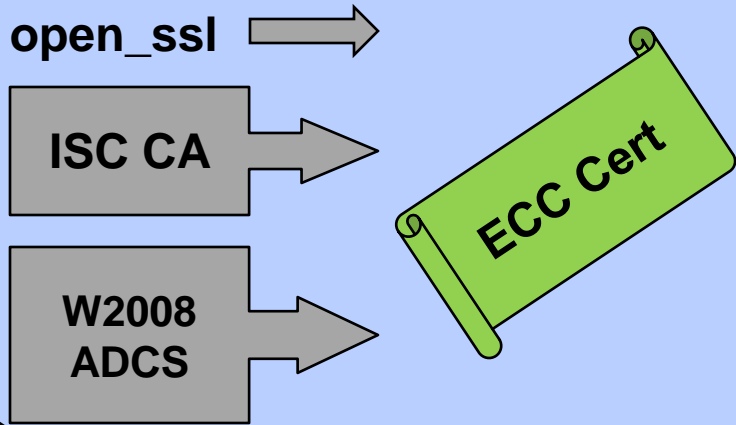
**Are You Ready for the Transition...!?**

# The Transition: Web Server

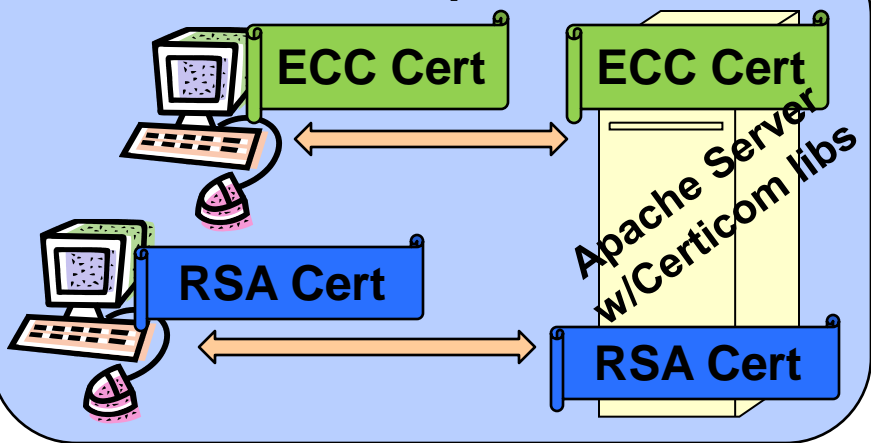


# MITRE Investigated ECC Technology

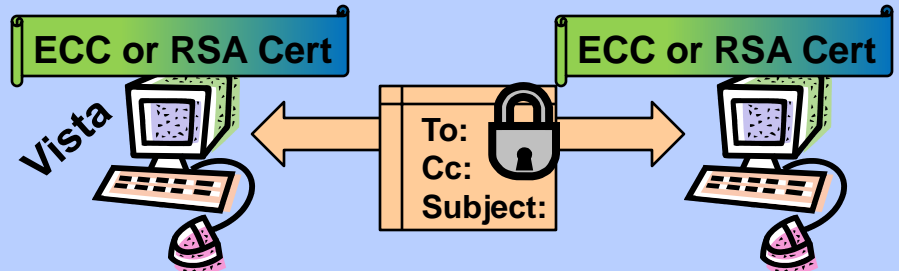
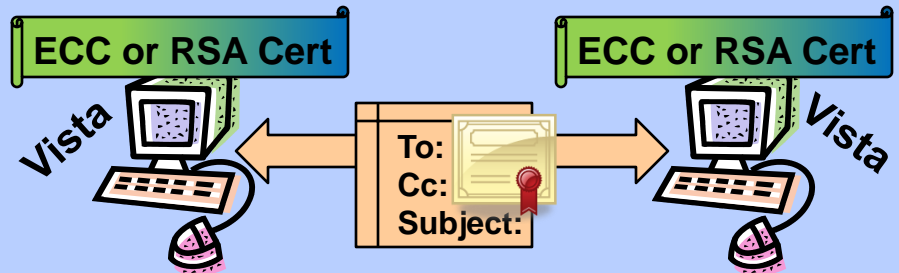
## Certificate Generation:



## ECC/RSA Compatible Server:



## Signed & Encrypted Email:



Outlook 2007

# Common Criteria SFRs & Cryptography

## ■ Affected by Cryptography

- Class FCS: Cryptographic Support
  - FCS\_CKM Key Management
  - FCS\_COP Cryptographic Operation
- Class FCO: Communication (Non-repudiation)
- Class FDP: User Data Protection
- Class FPR: Privacy
- Class FPT: Protection of the TSF

## ■ Not Affected by Cryptography

- Class FIA Identification and Authentication
  - When cryptographic keys are employed, use the class FCS

# The Future:

## A Simple Example: RSA Vs. ECC

### ■ RSA (Today):

- FCS\_CKM\_Example.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [PKCS #1 RSA Cryptography Standard]

### ■ ECC (Tomorrow):

- [RSA] → [ECC]
- [1024 bits] → [256 bits] → [secp256r1 or nistp256]
- [PKCS #1 RSA ..} → [SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography]

–

# ECC and Common Criteria

- **Schemes will continue to evaluate Quality of Crypto implementation**
  - **Paradigm Change**
    - **Same functionality using different building blocks**
  - **Need additional guidance and training**
- **Crypto evaluation considerations**
  - **Does TOE include Crypto? ECC, RSA, or other?**
  - **Is Crypto in the environment?**
  - **Is Crypto FIPS compliant or vendor affirmed?**
  - **Suite B Algorithms?**
- **Is Crypto / Environment in the Cloud?**
  - **A distributed environment**

# Questions ?

