



The 1998

RSA
Data Security
Conference™





RSA Directions & Products

Scott Schnell

Vice President · Marketing



Victor Chang

Vice President · Engineering



RSA Data Security



Agenda

- 🔑 Company update
- 🔑 Market update
- 🔑 Product announcements
- 🔑 Partner announcements
- 🔑 The year ahead



Company Update



RSA is the *de facto* industry standard for encryption technology and security software



RSA Data Security

Company Update



RSA technology licensed by 350 vendors



RSA Data Security

Company Update



RSA technology shipped in more than
300 million application copies



RSA Data Security

Company Update

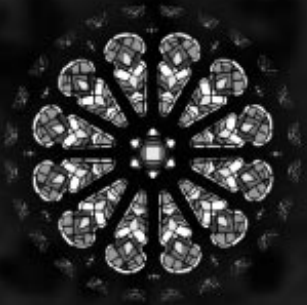


RSA technology specified in industry standards



RSA Data Security

Company Update



■ RSA OEMs focus on a variety of applications from the Internet to video and telecommunications

■ Signed new relationships with 74 companies, including...





RSA Mission

Expand and lead the market for software components that secure electronic data

Solve new and evolving problems in existing markets

Bring security benefits to new markets

Stay on the leading edge of technology



RSA Data Security



Security Market—Yesterday

Lightweight,
open applications,
e.g. Browsers

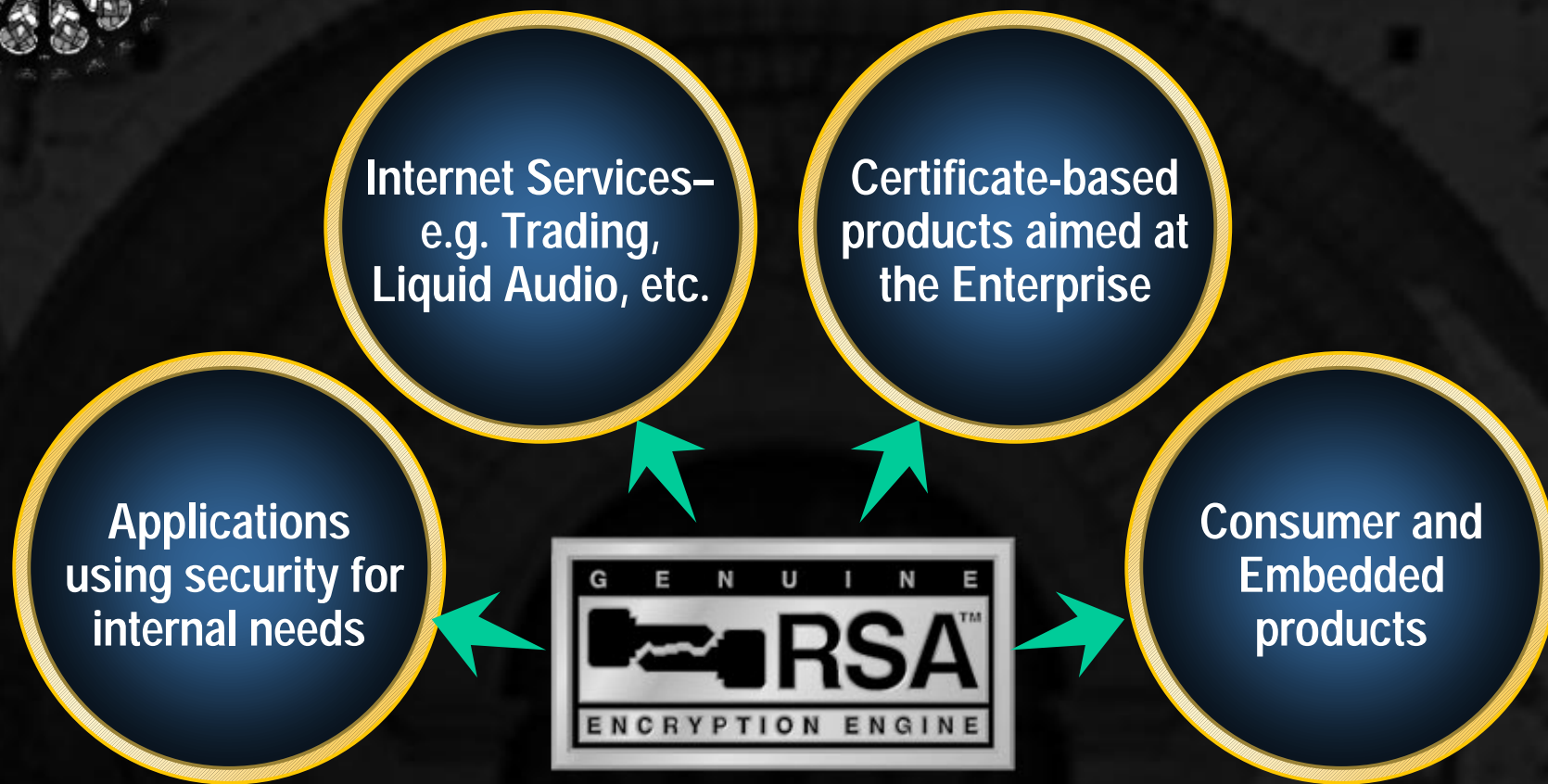
Heavyweight,
closed
applications,
e.g. Notes

- 🔑 PC-based
- 🔑 Security savvy developers
- 🔑 Early, obvious security-based features





Security Market—Today



RSA Data Security



Product Announcement

Field Trial of **BSAFE 4.0** includes

Elliptic Curve Cryptography

Elliptic Curve seeding program

- Goal is to get the product in the hands of 50 vendors by end of Q1
- Begin accepting applications NOW
- Code available in mid-February
- Free-of-charge



RSA Data Security



BSAFE 4.0

Features and Benefits

- 🔑 Elliptic Curve technology
- 🔑 BHAPI hardware API
- 🔑 X9 financial standards and FIPS support
- 🔑 Improved performance
- 🔑 First customer ship Q2 '98

Bsafe
THE CRYPTO TOOLKIT

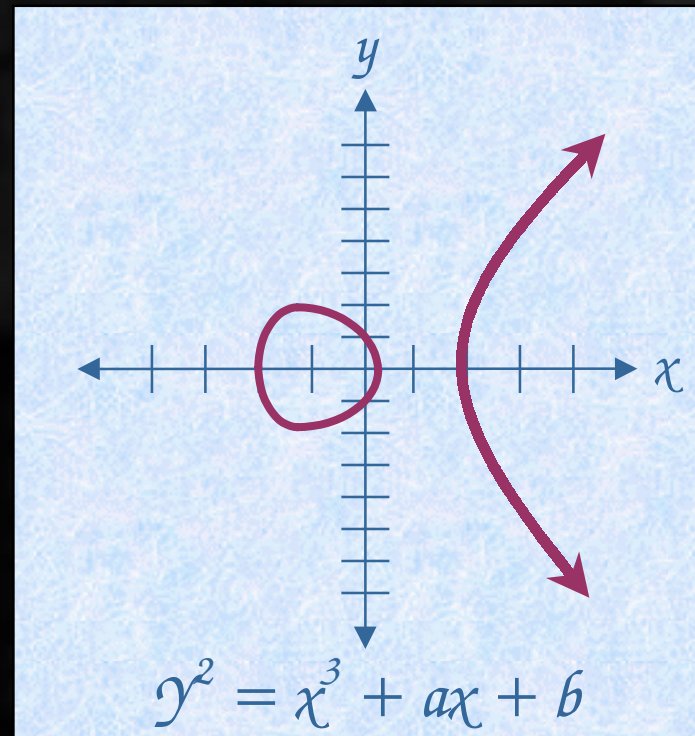


RSA Data Security



Elliptic Curve Cryptography Primer

- 🔑 A Public Key System
- 🔑 Three methods
 - Odd, Even-Normal, Even-Polynomial
- 🔑 Some appealing advantages, e.g., smaller key size
 - 160-bit ECC vs. 1024-bit RSA





ECC Myths and Facts

Myth

ECC method is "smaller"
than RSA method



RSA Data Security



ECC Myths and Facts

FACTS

- ECC **keys** are **smaller** than RSA keys
- In software, ECC **implementations** are actually somewhat **larger** than RSA





ECC Myths and Facts

Myth

ECC method is "faster"
than RSA method



RSA Data Security



ECC Myths and Facts

FACTS

- **ECC private key operations are faster** than RSA method
- **ECC public key operations are slower** than RSA method





ECC Myths and Facts

Myth

*Even-Normal ECC
method is "best" ECC
(vs. Odd and Even-Polynomial methods)*



RSA Data Security



ECC Myths and Facts

F A C T S

- *Even-Normal* ECC can be done in fewer silicon gates
- *Even-Normal* ECC is the **fastest** in hardware, but **slowest** in software
- *Odd* method leverages existing hardware and software implementations for RSA and Diffie Hellman techniques



ECC Implications

- Good for applications with little storage or low communication bandwidth
- Good for system applications without certificates
 - Avoid slow ECC signature verification
- Good where data “value” is more transitory



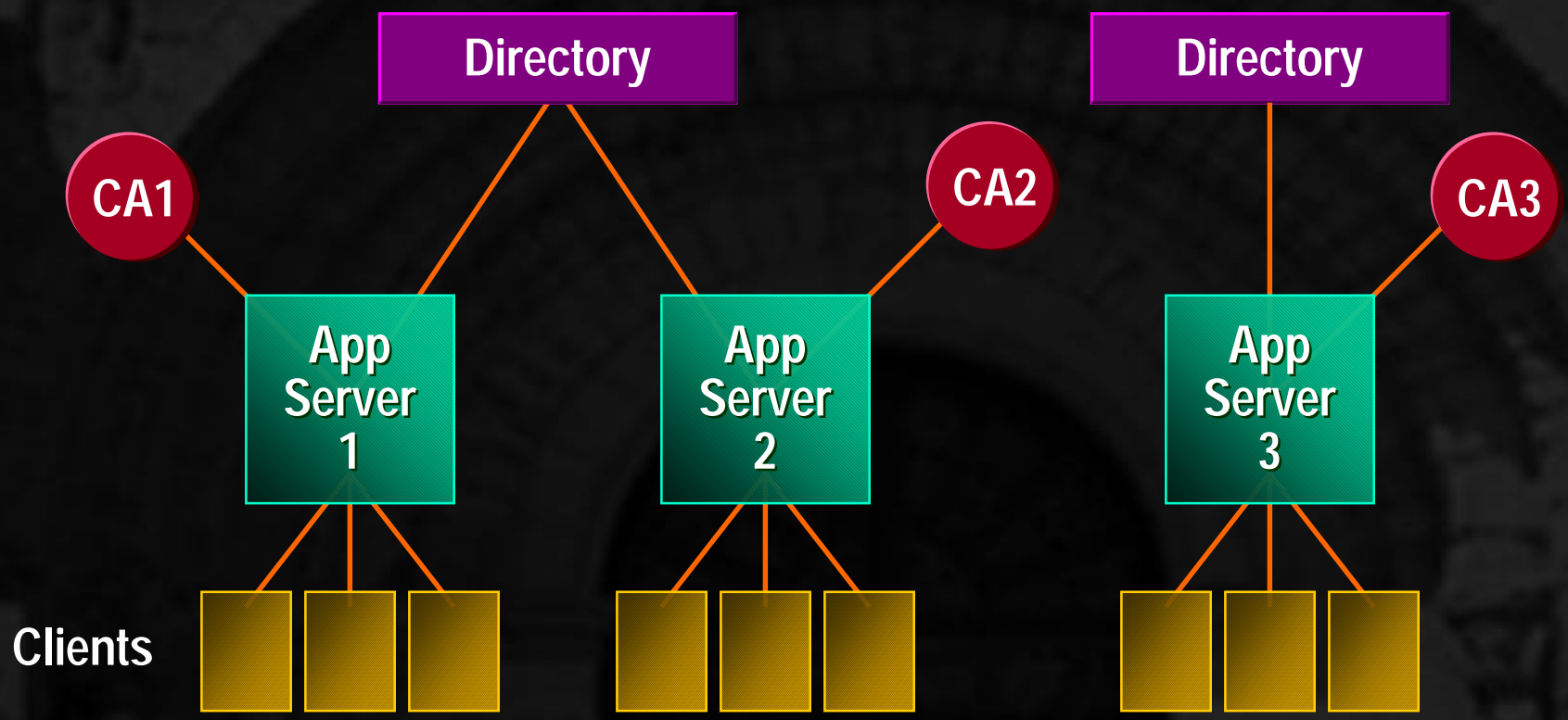


Security Market—Today





Certificate Management Today









Product Announcement

Certificate Security Suite

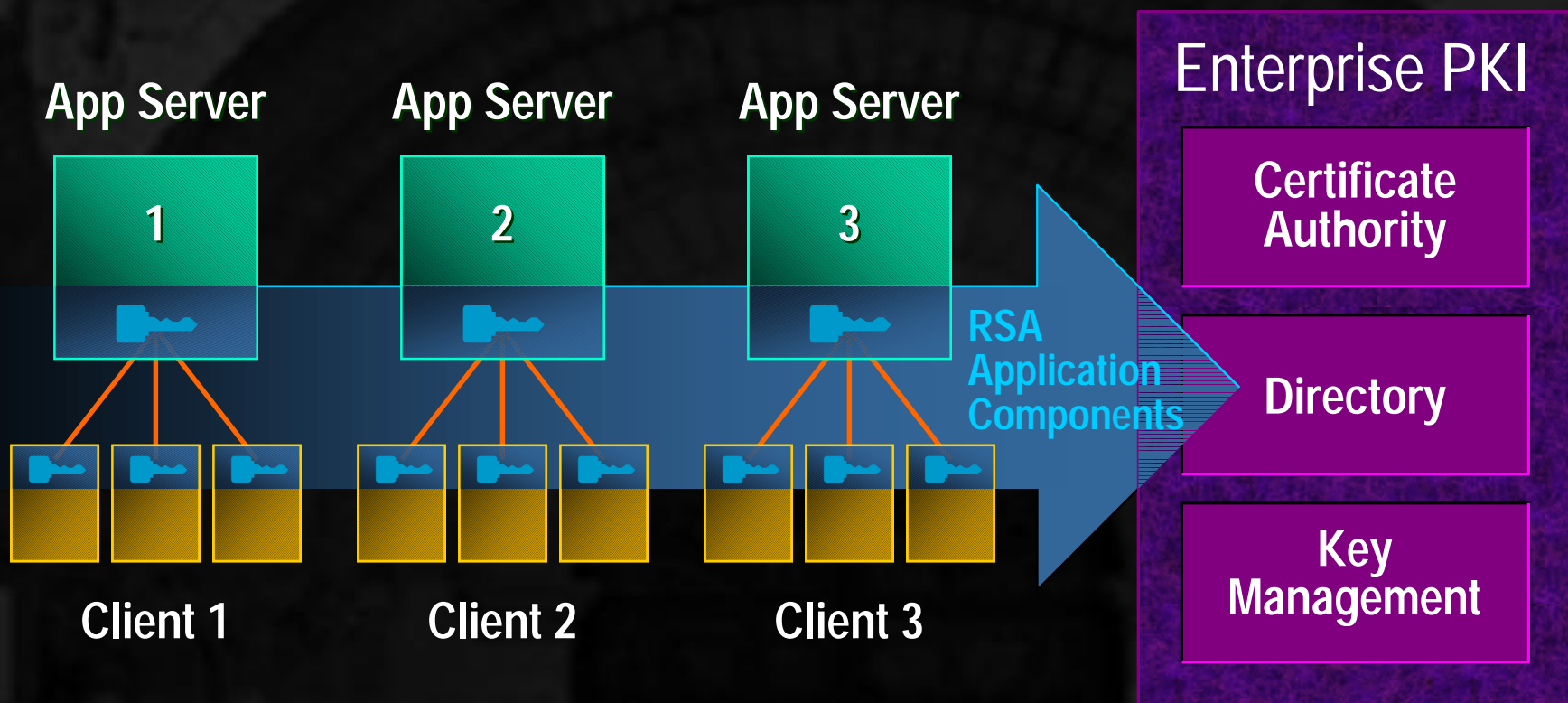
A set of high-level security components and tools with a shared API for Enterprise integration, designed for

-  Faster time to market
-  Reduced engineering costs
-  Decreased requirements for crypto expertise
-  Enhanced enterprise sales opportunities





The RSA Certificate Security Suite (CSS)



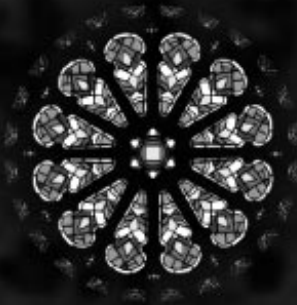
RSA Data Security



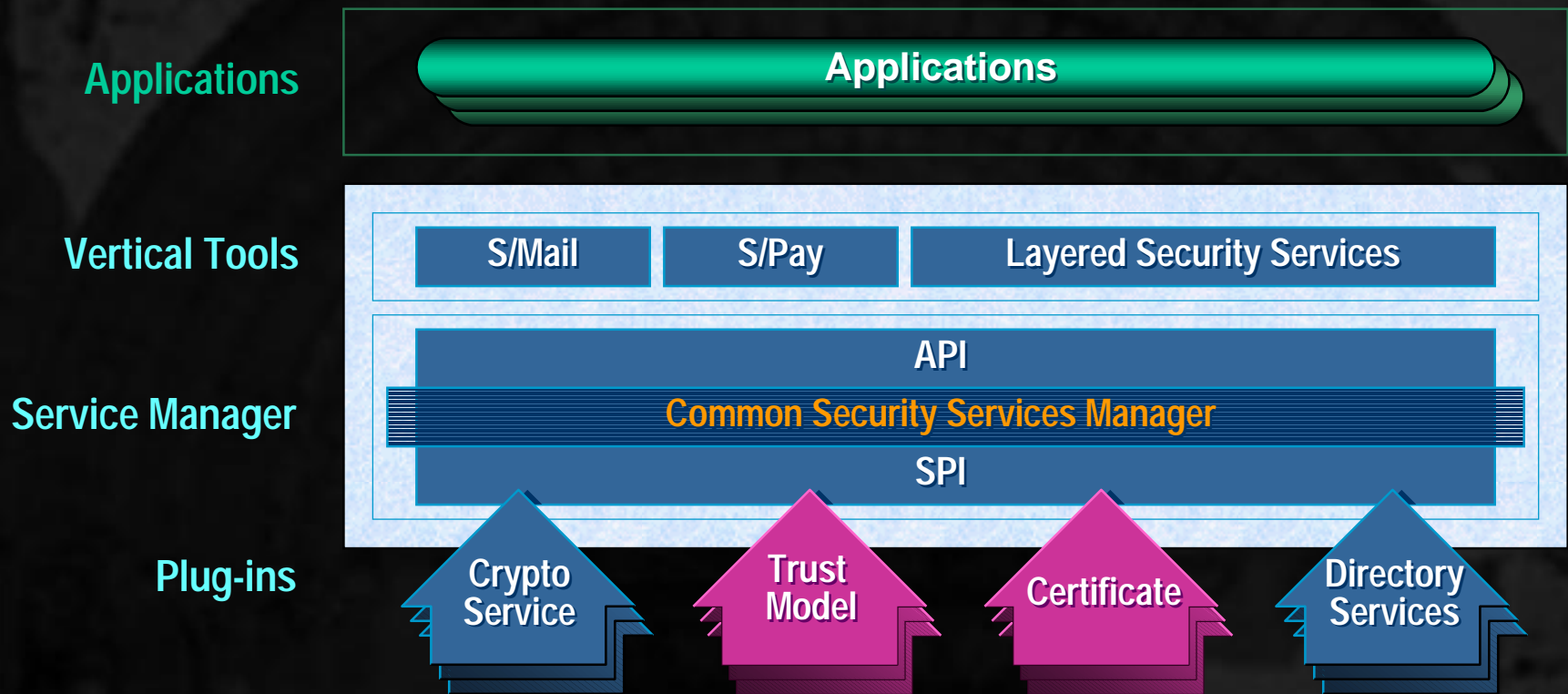
CSS 1.0 Features

- Supports X.509 v3 certificates
- Built-in crypto service providers
 - BSAFE CSP
 - PKCS#11 provider for smart cards
- Implements CDSA v1.2
- Built-in data libraries
 - ODBC
 - LDAP
- First customer ship Q2 '98





RSA's CSS Architecture



RSA Data Security



RSA and Phoenix

■ CryptoROM™

- PC authentication and security before operating system boot
- Genuine RSA Encryption Engine on PC OEM motherboards
- Accessible, standardized API

■ Learn more about CryptoROM in the Phoenix session and in the RSA booth

Phoenix[®]
Phoenix Technologies Ltd.



RSA Data Security



RSA – The Year Ahead

- Continue to innovate and lead in secure software technology
 - DES Challenge II commences today
 - RSA Labs PKCS #13



RSA Data Security



RSA – The Year Ahead

➤ Continuous customer satisfaction improvement



RSA Data Security



RSA – The Year Ahead

- Serve emerging consumer markets
 - Cable, pagers, cellular phones
 - μ BSAFE for constrained applications



RSA Data Security



RSA – The Year Ahead

- Extended line of certificate security components



RSA Data Security



RSA – The Year Ahead

- SET 1.0 compliance and new payment component options in S/PAY



RSA Data Security



RSA – The Year Ahead

- Continued leadership in Java security with JSAFE



RSA Data Security



The 1998

RSA
Data Security
Conference™

