EITC 2006
Portsmouth, NH

Excellence

in

Information

Technology

Compliance

Conference

March 29th & 30th

Session 2-2
Secure Communication
Are We There Yet?

Ramon Krikken, MSc CS, CISSP, CISA
Senior Consultant - NMI InfoSecurity Solutions

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

Introduction

- Customer information exchange
  - Business partners
  - Customers
- Email communication
  - Preferred communication medium
  - Non-secure – can be read and altered
  - Can be cryptographically secured
- Email encryption
  - Implemented in most email clients
  - S/MIME and PGP are accepted standards

- So why is encrypted email not widely used?

EITC 2006
Portsmouth, NH

Excellence

in

Information

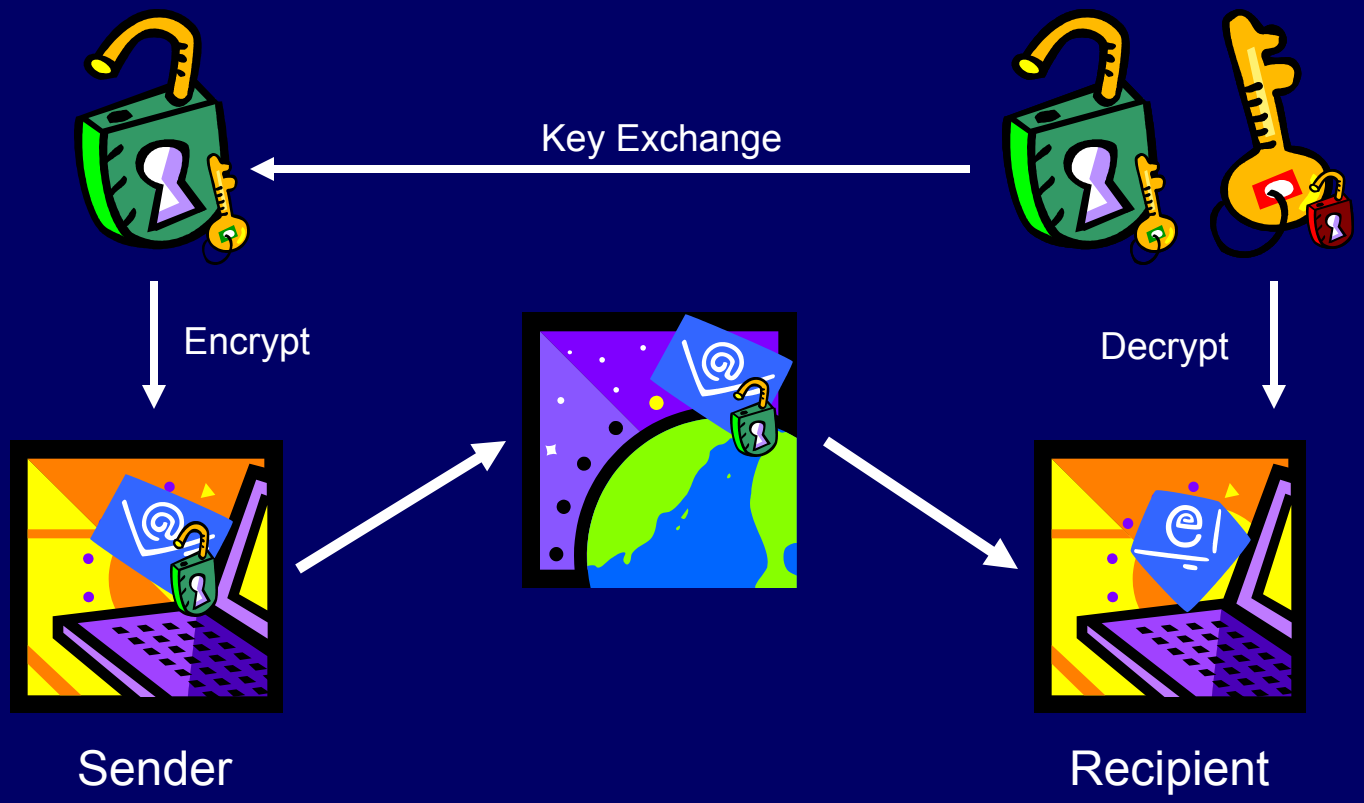
Technology

Compliance

Conference

March 29th & 30th

Email Encryption Simplified



EITC 2006
Portsmouth, NH

Excellence

in

Information

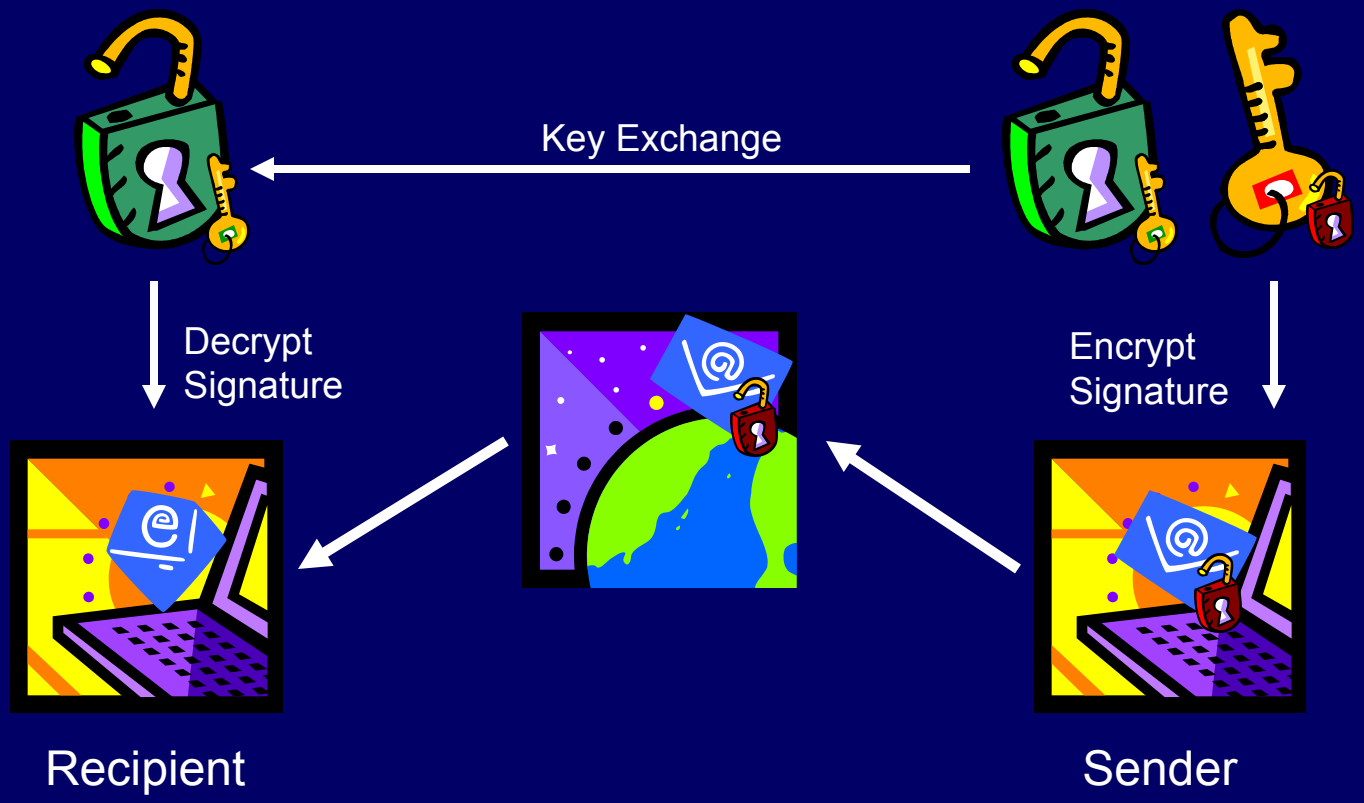
Technology

Compliance

Conference

March 29th & 30th

Email Signing Simplified



It Seems Simple, But …

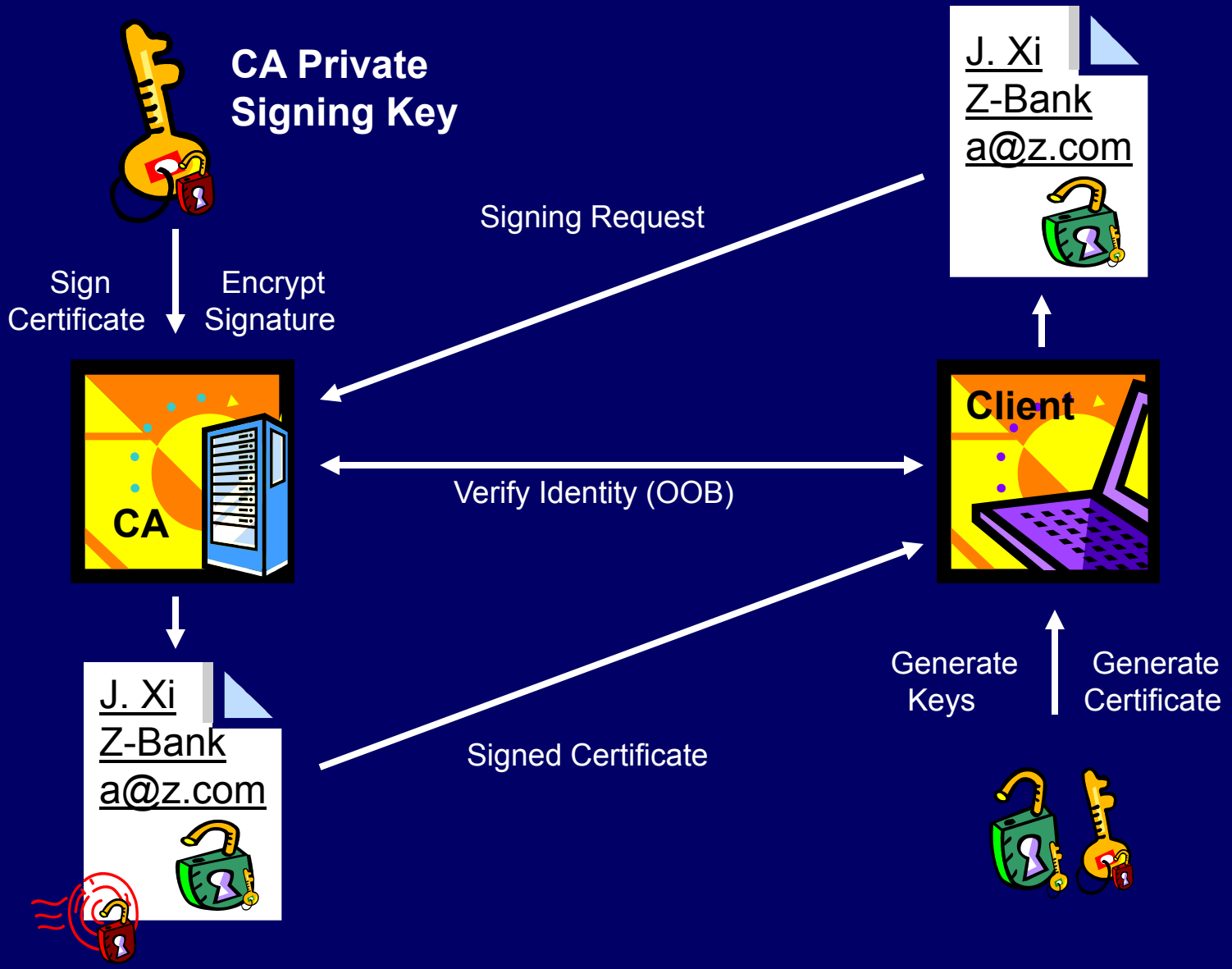
- Email encryption and signing are simple operations
  - All the sender needs is the recipient public key
- Key management and Identity management are not
  - Recipient is responsible for key/ID generation
  - What happens if the recipient loses the keys?
  - What happens if the private key is stolen?
  - How to exchange the public key securely?
  - How to know that the public key belongs to the right person?
- Enter: PKI – Public Key Infrastructure

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

Identity Management Simplified

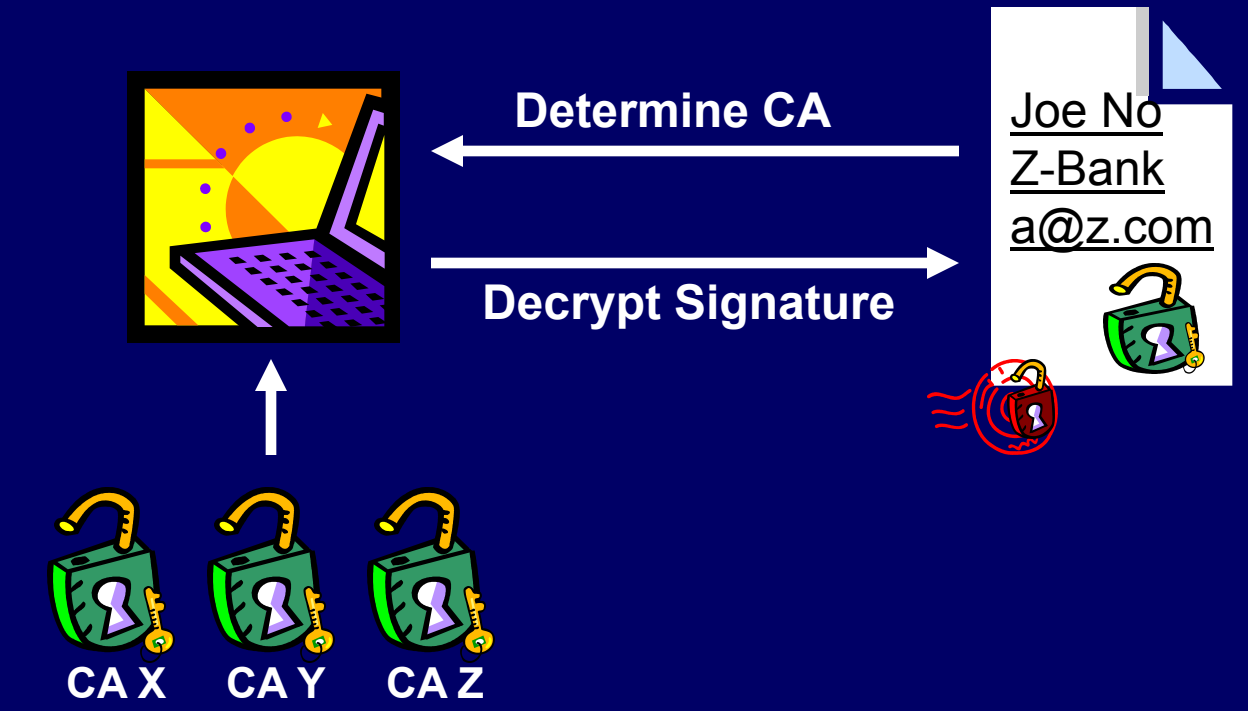


EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

Identity Management Simplified



Still Seems Rather Simple?

- Certificate signing concept is simple operation
  - Just have a trusted party validate and sign
- Real-world implementation is not so simple
  - Recipient knowledge of PKI required for request and management of certificates
  - Both recipient and sender must trust the CA
  - Universally accepted CAs are commercial entities (cost of signing)
- Solutions other than commercial CAs exist but are more complex (cross-signing institutional CAs, Web of Trust)
- This is why PKI has not caught on (yet)

More Complications

- Design of email encryption standards do not support business requirements
- S/MIME and PGP put users in control of keys, content and policy, but business needs:
  - Enterprise virus and content scanning
  - Email archiving for certain content
  - Email access after employee leaves
- Design of email encryption standards do not support technology-illiterate users
  - Recipient (i.e. business partner or customer) responsible for managing identities and keys

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

Stop-Gaps Don't Work

- Password-protected documents
  - Dependent on password strength
  - May use proprietary (weak?) encryption
  - Not all documents support passwords
- Encrypted ZIP file
  - More convenient than documents
  - Strong encryption supported
  - Dependent in password strength
  - File listing not encrypted
  - Blocked in email by most organizations

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

The Appliance - A Solution?

- Several secure email appliances exist. Features are:

- In DMZ to intercept Internet email
- Encryption on appliance, not desktop
- Delivery via S/MIME or SSL browser
- Automatic policy-based encryption
- Automatic S/MIME certificate gathering
- Simple recipient identity management

EITC 2006
Portsmouth, NH

Excellence

in

Information

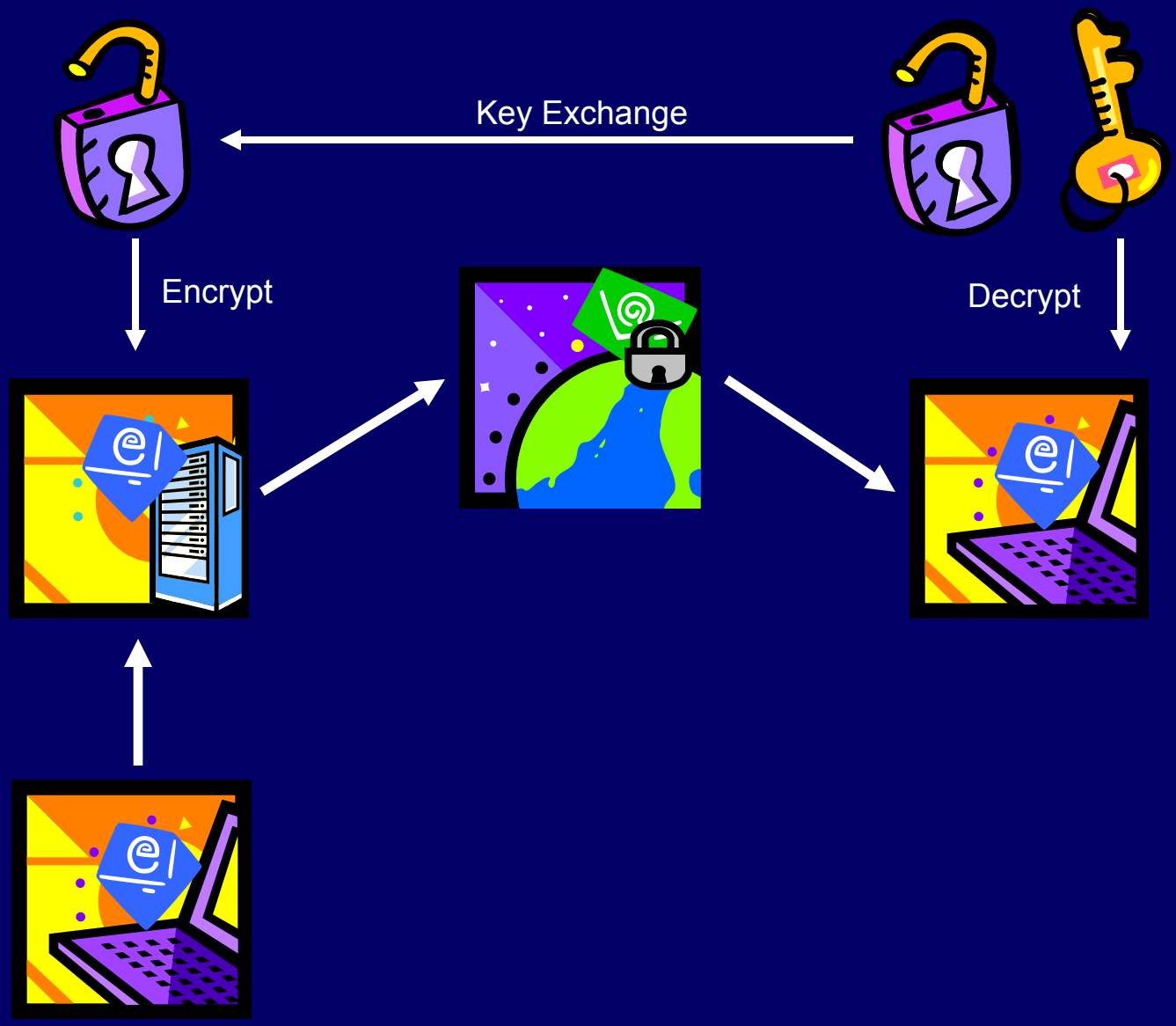
Technology

Compliance

Conference

March 29th & 30th

Secure Email Appliance

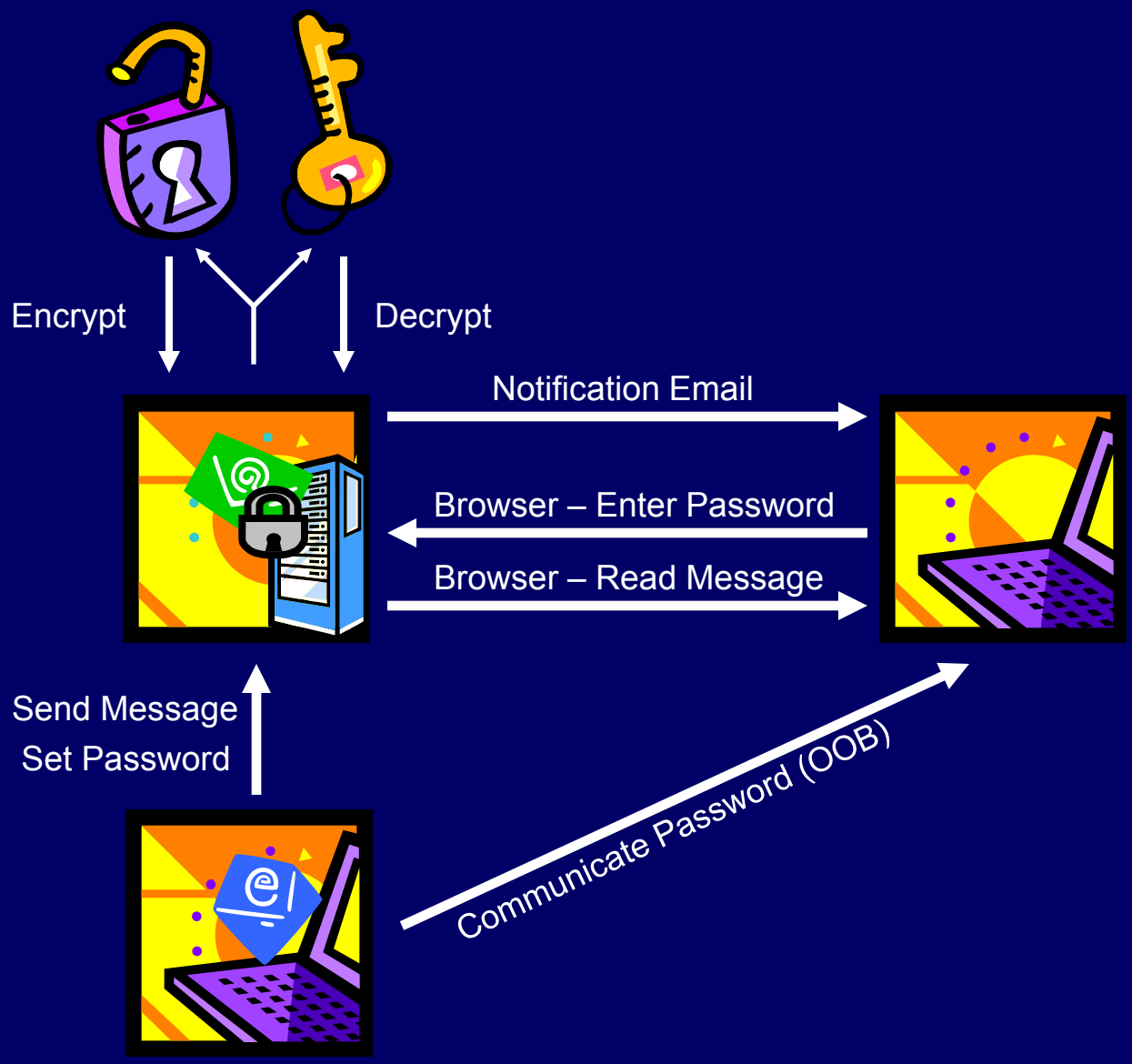


EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

Secure Email Appliance



EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

The Appliance - A Solution?

- Advantages
  - Enterprise control over keys and policy
  - Can use network virus and spam control
  - No software interoperability issues
- Disadvantages
  - No end-to-end encryption, limited usability for intranet communication
  - Browser-based communication is clunky
  - Unencrypted and unsigned notification email can be intercepted or falsified

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

So Are We There Yet?

- Technically: Maybe
  - S/MIME/PGP can be used with business partners - if both parties use the same
  - Appliance can be used with anyone
- Culturally: Maybe not just yet
  - All solutions have a learning curve for recipient as well as sender
  - Cryptography misunderstood by many, resulting in false sense of security
- But it has to start somewhere

EITC 2006
Portsmouth, NH

Excellence in Information Technology Compliance Conference

March 29th & 30th

And A Final Word of Warning

- Unlearning the anti-phishing lesson?
  - Bank could use encrypted email for sending notifications to customers
- The 'SSL lock icon' syndrome
  - Encryption/signing credentials not necessarily checked – can be technically difficult
  - Any encryption/signing seen as proof that bank sent the email – false sense of trust
- Appliance doesn't necessarily solve this
  - The notification email can be falsified
- Could be a step back in combating fraud?