JAVA DAYS ´99



Java™ Cryptography Architecture

Gary Ellison
Senior Security Engineer
Sun Microsystems

Sun microsystems

Presentation Outline



- Design principles
- Architecture overview
- Unique crypto features
- Questions & Answers

© 1999 Sun Microsystems GmbH

Sun microsystems

Design Principles

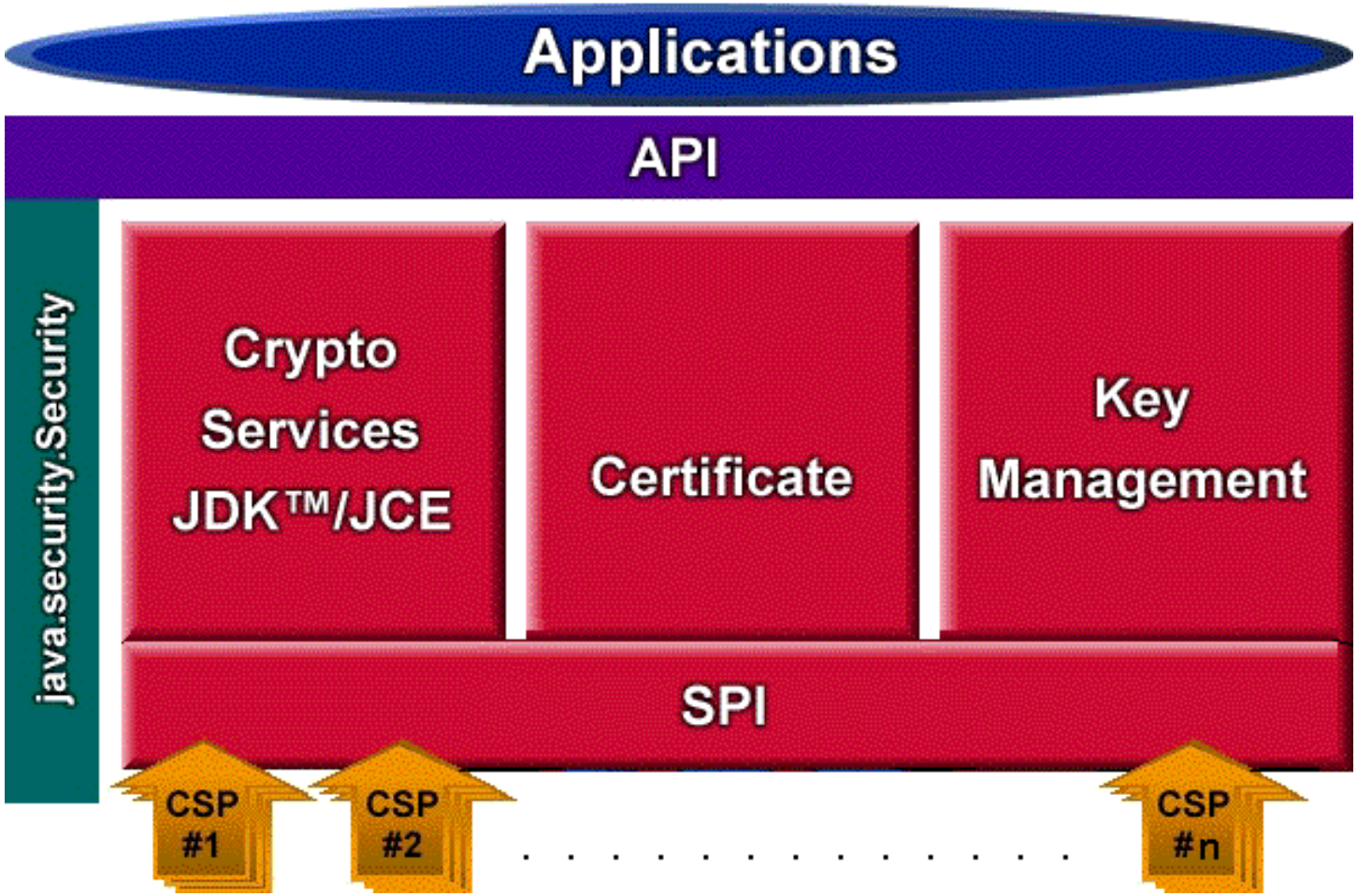


- Implementation independence
  - Providers
- Algorithm independence
  - Engine classes
- Interoperability

© 1999 Sun Microsystems GmbH

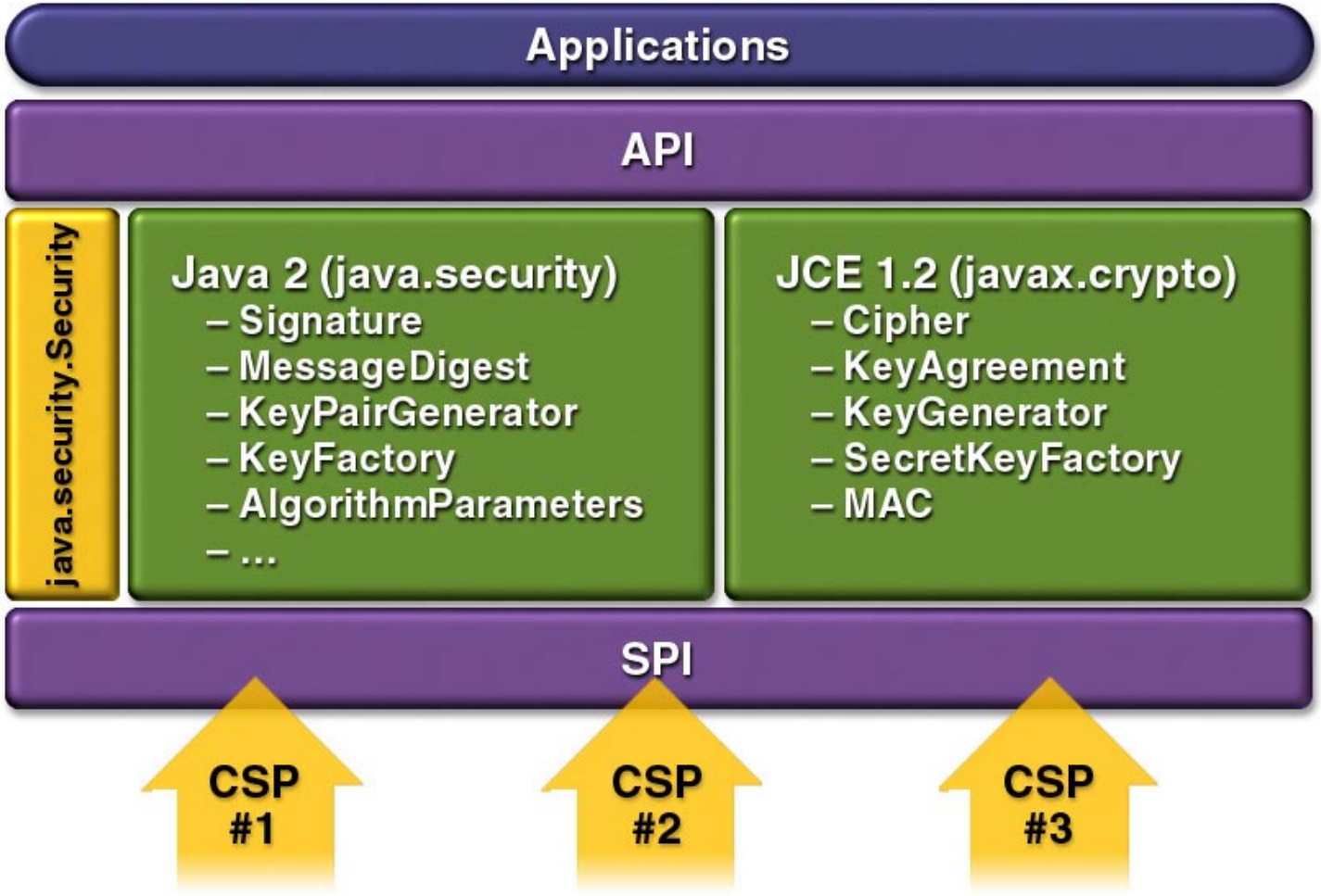
Sun microsystems

Architecture Overview



© 1999 Sun Microsystems GmbH

Java Cryptography Architecture



© 1999 Sun Microsystems GmbH

JDK™ API Built-In Algorithms



- MD5
- SHA1
- SHA1 with DSA
- SHA1 with RSA (JDK™ 1.3)
- MD2 with RSA (JDK™ 1.3)
- MD5 with RSA (JDK™ 1.3)

© 1999 Sun Microsystems GmbH

Sun microsystems

Java™ Cryptography Extension (JCE) 1.2 API

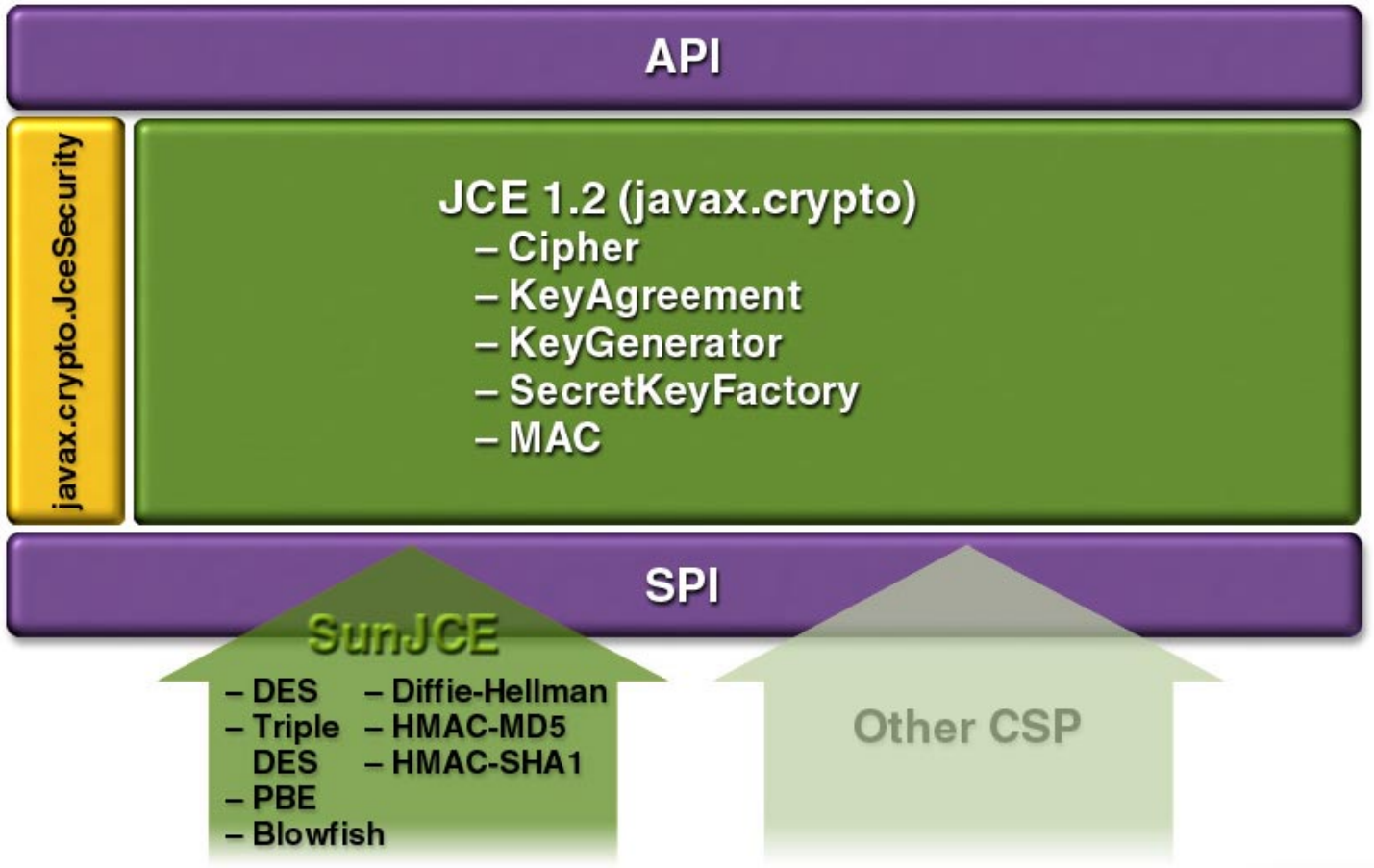


- Standard extension (javax.crypto)
- Entirely written in the Java™ programming language
- Binaries are not exportable

© 1999 Sun Microsystems GmbH

Sun microsystems

SunJCE 1.2 API Built-In Algorithms



© 1999 Sun Microsystems GmbH

Encryption Example



- // Generate random session key

```
KeyGenerator kgen = KeyGenerator.getInstance("DES");
SecretKey sKey = kgen.generateKey();
```

- // Create and initialize cipher

```
Cipher c = Cipher.getInstance("DES", "SunJCE");
c.init(Cipher.ENCRYPT_MODE, sKey);
```

- // Encrypt data

```
byte[] clearText = "abcdef".getBytes();
byte[] cipherText = c.doFinal(clearText);
```


© 1999 Sun Microsystems GmbH

Sun microsystems

Key Factory





```
byte[ ] y={..};
byte[ ] p={..};
byte[ ] q={..};
byte[ ] g={..};
```


© 1999 Sun Microsystems GmbH

Key Factory Example



- // Key material for DSA public key

```
y = new BigInteger(...);
p = new BigInteger(...);
q = new BigInteger(...);
g = new BigInteger(...);
```

- // Create key specification

```
DSAPublicKeySpec spec = new DSAPublicKeySpec(y, p, q, g);
```

- // Create PublicKey object and use it

```
KeyFactory kfac = KeyFactory.getInstance("DSA");
PublicKey dsaPubKey = kfac.generatePublic(spec);
```


© 1999 Sun Microsystems GmbH

KeyStore



- Repository of credentials
- Private keys include certificate chain to authenticate public key
- Stream-based storage and retrieval
- Password-protected
- Fully customizable
  - Abstract class

    java.security.KeyStore
- Managed by keytool utility

© 1999 Sun Microsystems GmbH

Sun microsystems

Certificate and CRL Support



- java.security.cert package
- Instantiation through certificate factories
- Built-in implementation follows IETF PKIX profile (part 1)

© 1999 Sun Microsystems GmbH

Certificate Example




```
// Create input stream
  fis = new FileInputStream("pkcs7");
// Get an instance of a CertificateFactory
  cf = CertificateFactory.getInstance("X.509");
// Parse all the certificates in the InputStream
  Collection c = cf.generateCertificates(fis);
// Process the certificates
  Iterator i = c.iterator();
  while (i.hasNext()) {
     Certificate cert = (Certificate)i.next();
  }
```


© 1999 Sun Microsystems GmbH

Sun microsystems

Cryptography Features Unique to the Java™ Platform

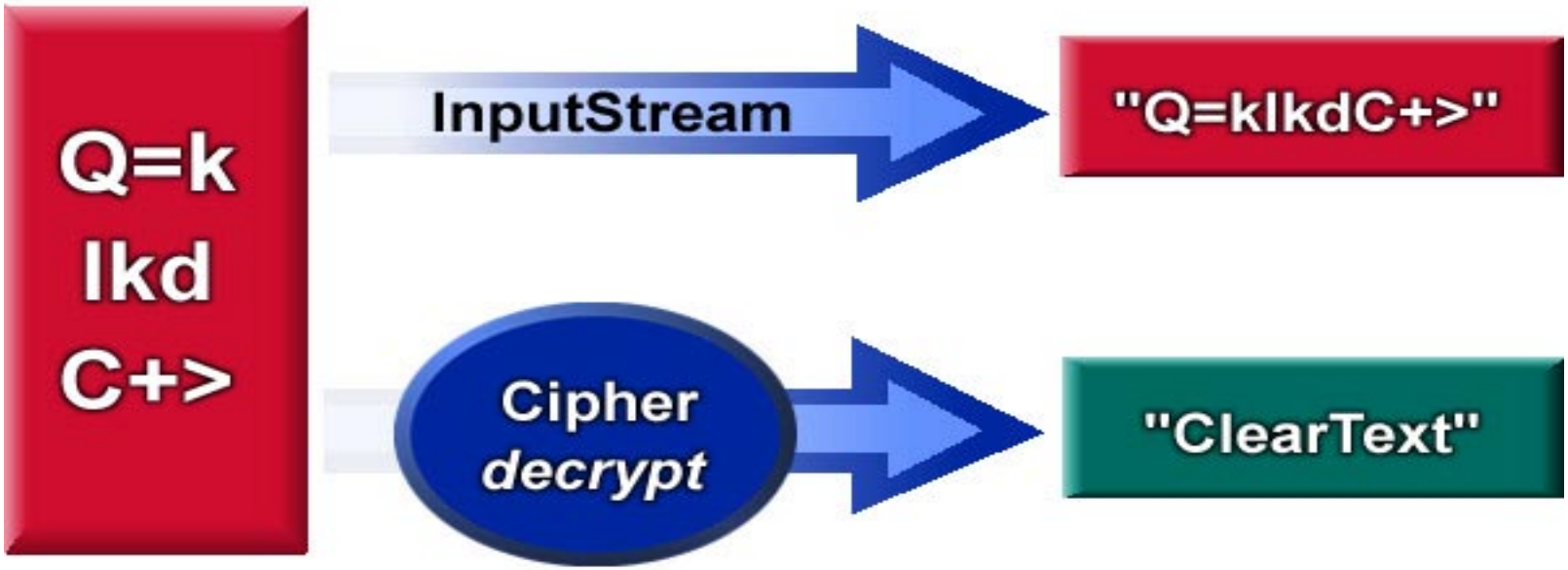


- Secure streams
  - CipherInputStream
  - CipherOutputStream
- Secure objects
  - SignedObject
  - SealedObject

© 1999 Sun Microsystems GmbH

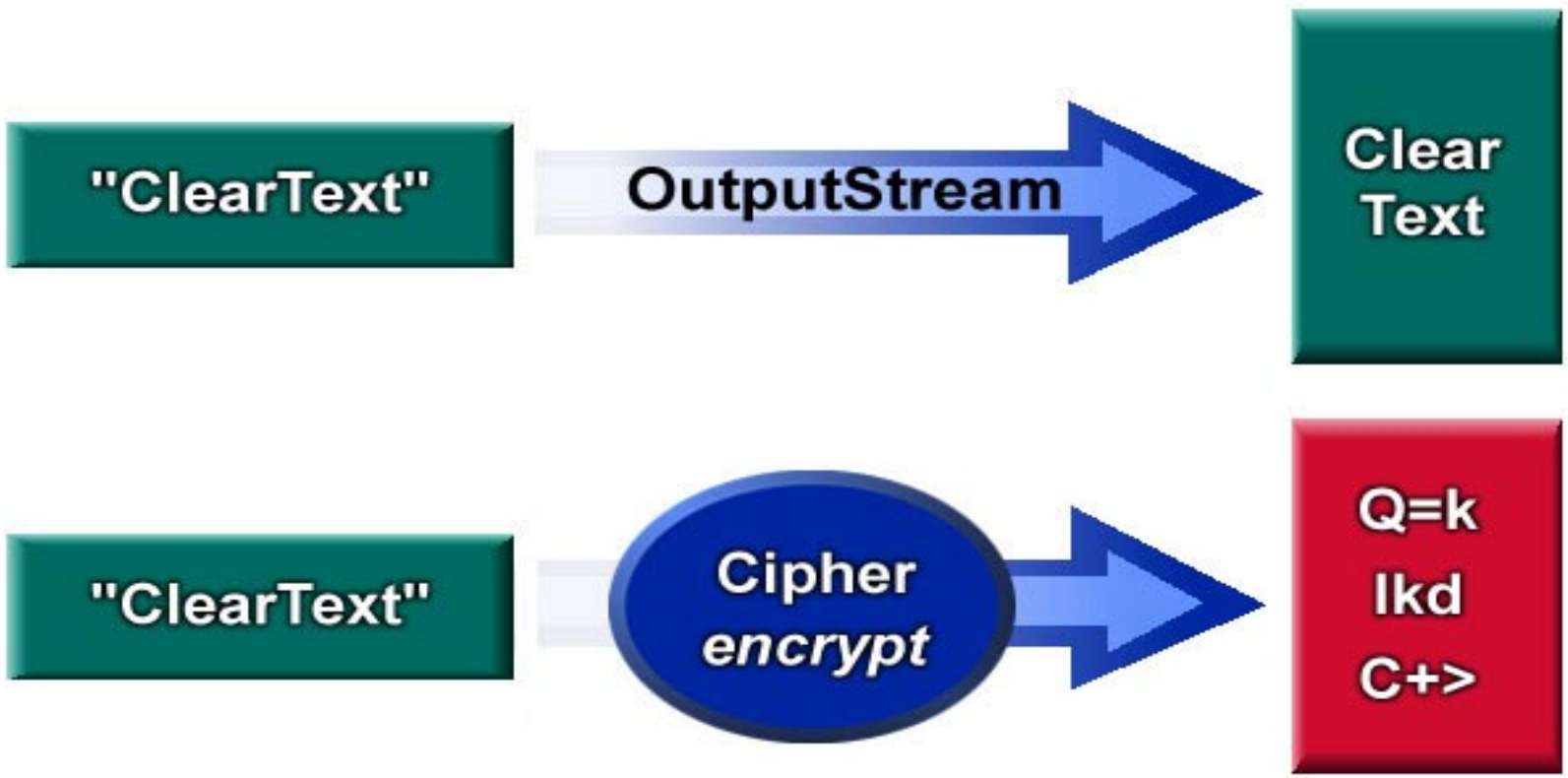
Sun microsystems

CipherInputStream



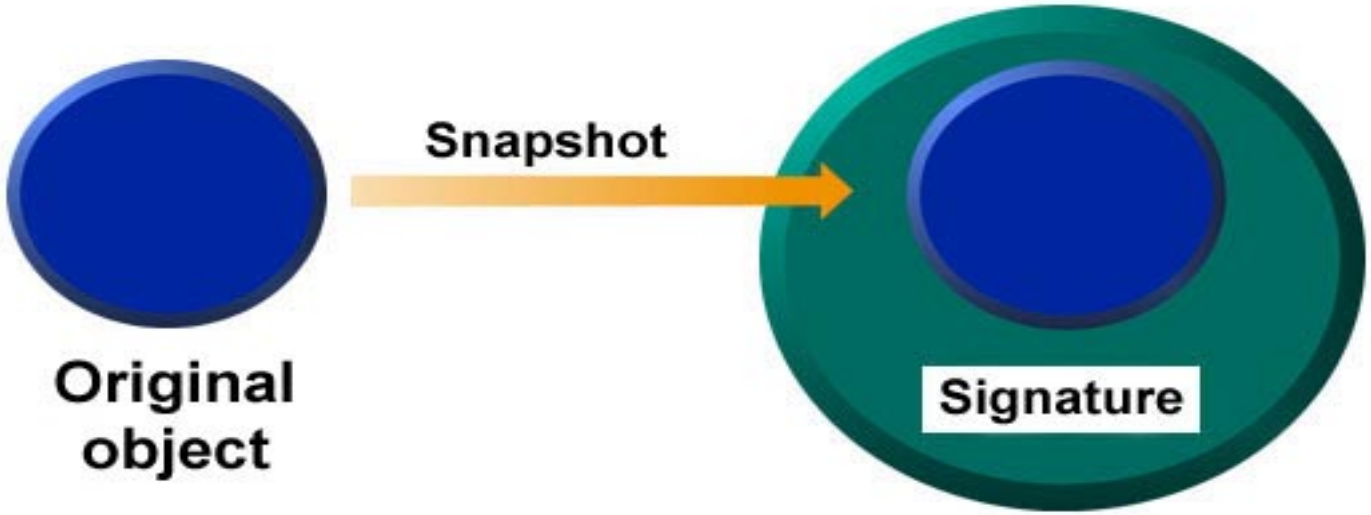
© 1999 Sun Microsystems GmbH

CipherOutputStream



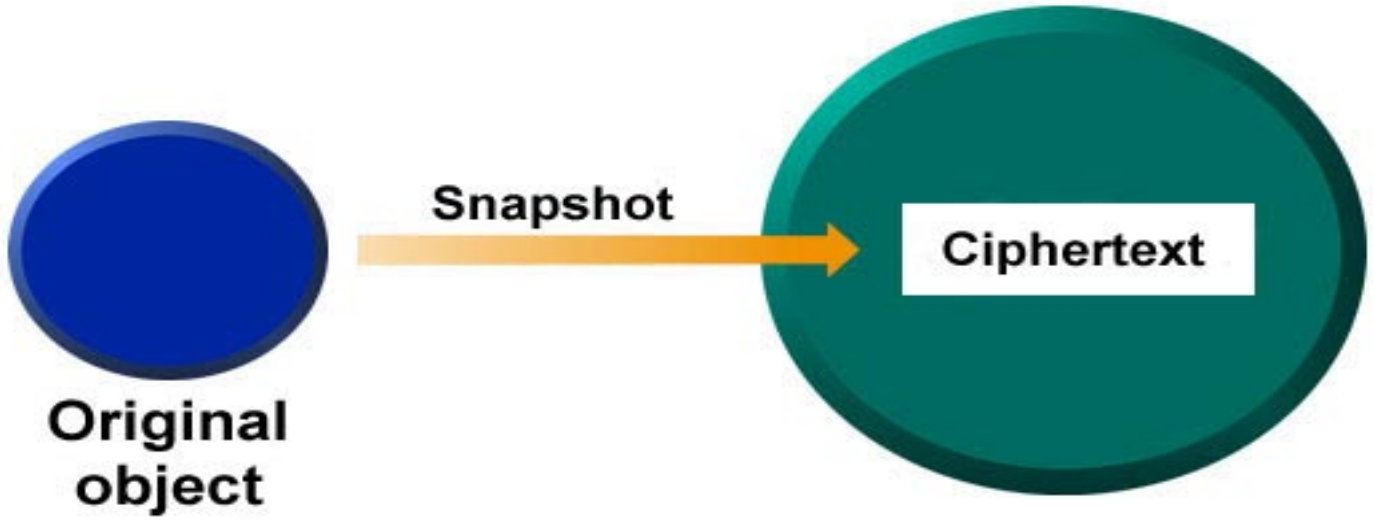
© 1999 Sun Microsystems GmbH

SignedObject



© 1999 Sun Microsystems GmbH

SealedObject



© 1999 Sun Microsystems GmbH

Conclusion



- We offer you a security toolkit that is
  - Powerful
  - Flexible
  - Complete
  - Easy-to-use

© 1999 Sun Microsystems GmbH

Sun microsystems

Future Work



- Performance speed-up

  (Java™ HotSpot™ VM)

- We are working towards adding
  - Provider authentication
  - Exportable JCE version

© 1999 Sun Microsystems GmbH

Sun microsystems

Looking For More Information?



- JDK™ 1.2 API and JCE 1.2 API
  - http://java.sun.com/jdc
  - http://java.sun.com/products/jce
- CSPs and Clean Room Implementations
  - http://java.sun.com/products/jce/jce12_providers.html
  - RSA DSI http://www.rsa.com/rsa/products/jsafe
  - Australian Business Access http://www.aba.net.au/solutions/crypto/jce.html
  - Forge Research http://www.forge.com.au
  - DSTC http://security.dstc.edu.au/projects/java/release3.html
  - IAIK http://jcewww.iaik.tu-graz.ac.at/jce/jce.htm
  - Entrust Technologies http://www.entrust.com/toolkit/java
  - Baltimore http://www.baltimore.ie/products/jcrypto

© 1999 Sun Microsystems GmbH



© 1999 Sun Microsystems GmbH