Enabling Grids for E-science in Europe

Information Society Technologies

Security and Certification; Authentication and Authorisation

John Kewley

EGEE is funded by the European Union under contract IST-2003-508833

Enabling Grids for E-science in Europe

Information Society Technologies

Security and Certification; Authentication and Authorisation

EGEE Training Team

EGEE is funded by the European Union under contract IST-2003-508833

Acknowledgements

- Some of these slides have been taken from a longer presentation by Mike Jones of the University of Manchester.
- Prepared by John Kewley, CCLRC Daresbury Laboratory

Enabling Grids for E-science in Europe

Goals of this module

Describe …

- Security basics
- Use of Certificates
- Importance of Certificate Authorities

Enabling Grids for E-science in Europe

Overview

- Introduction to Security
- Public/private keys in action
- Certificates
- Certificate Authorities

Introduction to Security

What aspects of security should we be concerned about?

- Authentication (Identification)
- Confidentiality (Privacy)
- Integrity (non-Tampering)
- Authorisation

Also

- Accounting
- Delegation
- Non-Repudiation

Tools of the trade

- Encryption
  - Secret “symmetric” key – both parties need to share the key
    - DES, RC4
    - Comparatively efficient
  - Public/private key – “asymmetric” - 2 keys mathematically related
    - RSA, DSA
    - Slower
- Oneway hash / message digest
    - MD5, SHA-1
    - fast

Gbbyf bs gur genqr

- Rapelcgvba
  - Frpergt “flzzrgevp” xrl – obgu cnegvrf arrq gb funer gur xrl
    - QRF, EP4
    - Pbzcnengviryl rssvpvrag
  - Choyvp/cevingr xrl – “nflzzrgevp” - 2 xrlf zngurzngvpnyyl eryngrq
    - EFN, QFN
    - Fybjre
- Barjnl unfu / zrffntr qvtrfg
    - ZQ5, FUN-1
    - Snfg

Tools of the trade

- Encryption
  - Secret “symmetric” key – both parties need to share the key
    - DES, RC4
    - Comparatively efficient
  - Public/private key – “asymmetric” - 2 keys mathematically related
    - RSA, DSA
    - Slower
- Oneway hash / message digest
    - MD5, SHA-1
    - fast

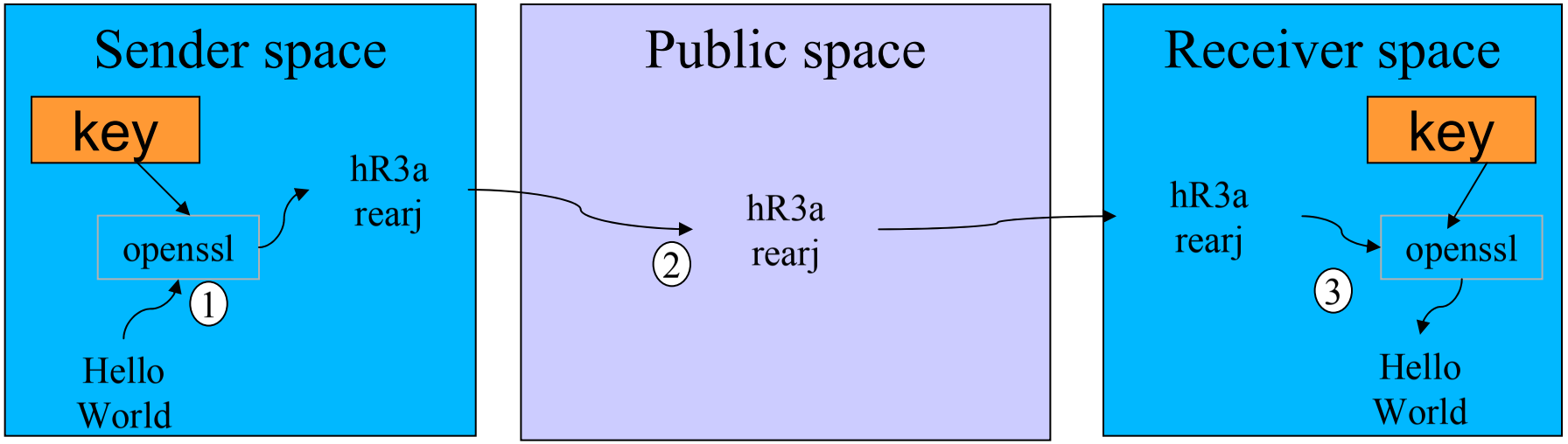
Encrypting for Confidentiality (1)

Sending a message using symmetric keys

1. Encrypt message using shared key
2. Send encrypted message
3. Receiver decrypts message using shared key

Only someone with shared key can decrypt message

But how do the keys get shared?

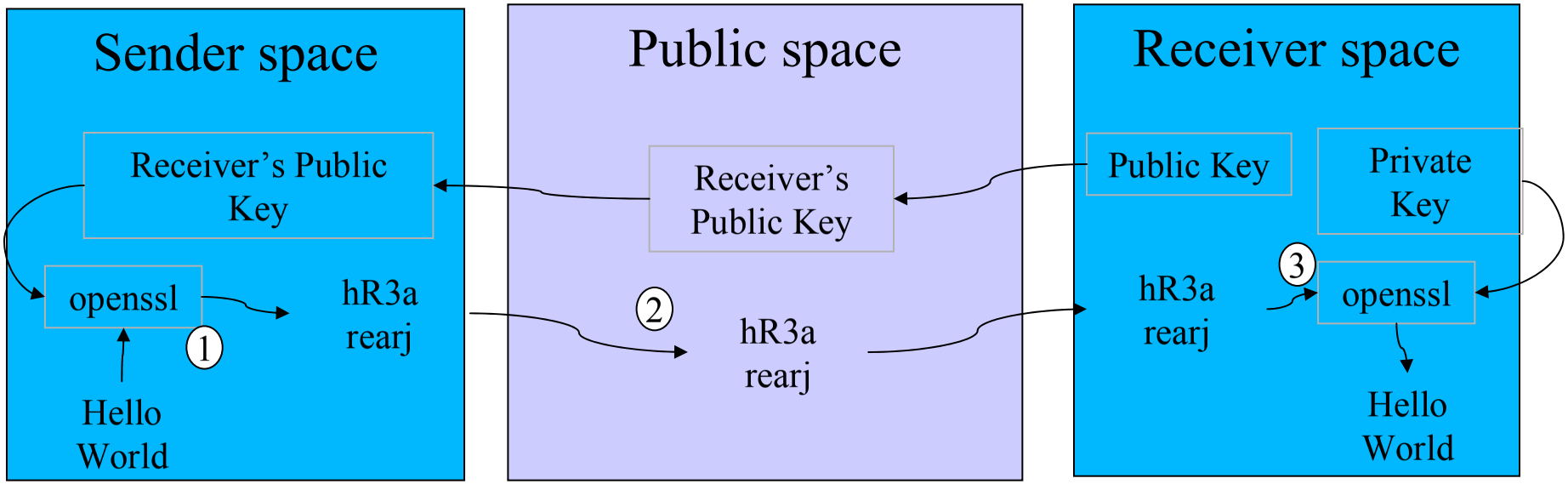


Encrypting for Confidentiality

Sending a message using asymmetric keys

1. Encrypt message using Receiver's public key
2. Send encrypted message
3. Receiver decrypts message using own private key

Only someone with Receiver's private key can decrypt message

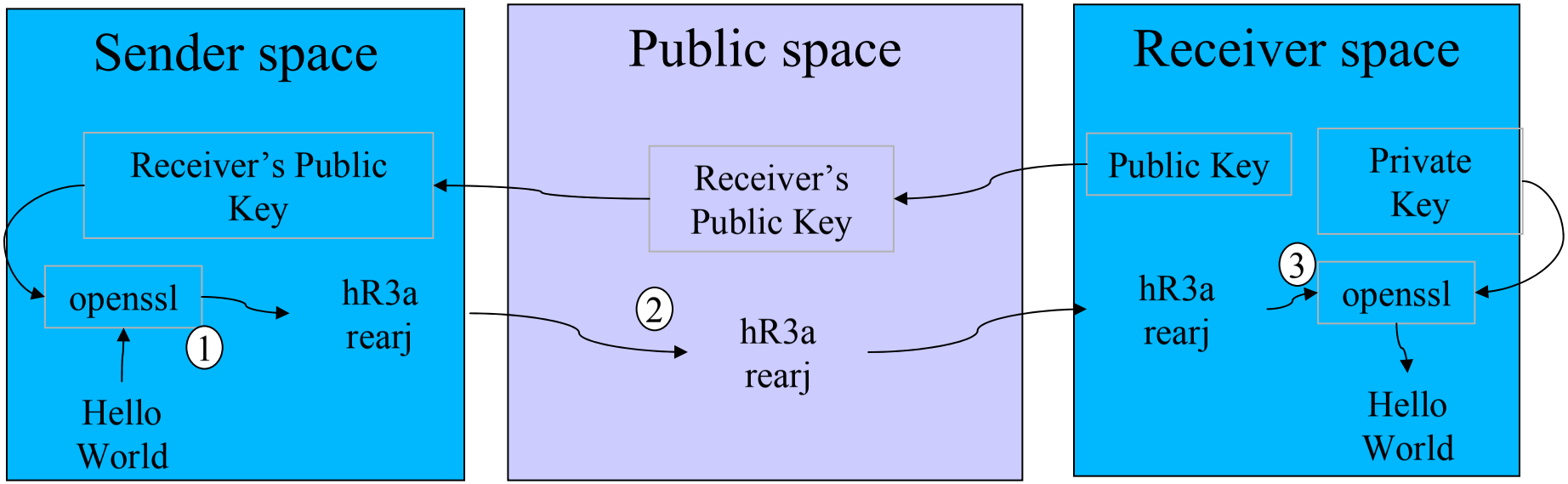


Encrypting for Confidentiality (2)

Sending a message using asymmetric keys

1. Encrypt message using Receiver's public key
2. Send encrypted message
3. Receiver decrypts message using own private key

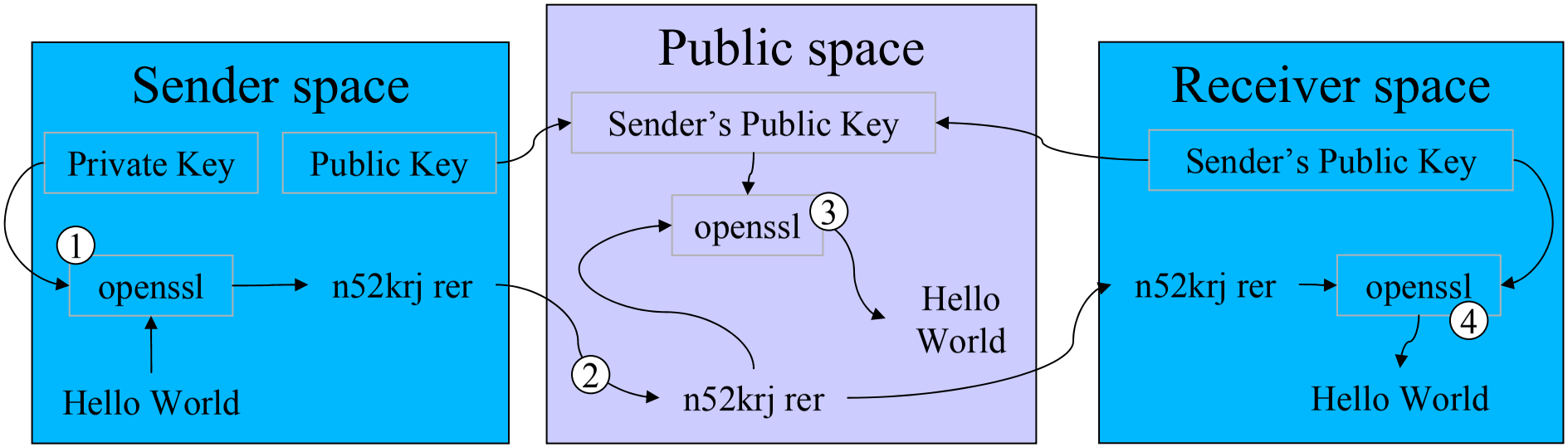
Only someone with Receiver's private key can decrypt message



Signing for Authentication

1. Encrypt message with Sender's private key
2. Send encrypted message
3. Message is readable by ANYONE with Sender's public key
4. Receiver decrypts message with Sender's public key

Receiver can be confident that only someone with Sender's private key could have sent the message



Certificates

- A statement from someone else (the Certificate Authority), that your public key (and hence your private key) is associated with your identity
- A certificate can be checked if you have the public key of the party who signed it

Certificate Authority

- A Certificate Authority (CA) issues you your certificates.
- By signing them it is able to vouch for you to third parties
- In return for this service, you must provide appropriate documentary evidence of identity when you apply for a certificate through a Registration Authority (RA)

Certificate contents

- The certificate that you present to others contains:
  - Your distinguished name (DN)
  - Your public key
  - The identity of the CA who issued the certificate
  - Its expiry date
  - Digital signature of the CA which issued it

The Full Monty

- Server authenticates Client
- Client authenticates Server
- (Symmetric) Session key exchanged confidentially using public key mechanism
- Secure session can now commence using more efficient, agreed “session key”
- Secure messages will also contain a message digest to ensure integrity

Summary

We have looked at

- Security basics
- Use of Certificates
- Importance of Certification Authorities