



# DIGITAL SIGNATURES SIMPLY EXPLAINED

Compiled and Presented by

**John Daly**  
**Senior Consultant**  
**Critical Path Asia Pacific**



## Authentication and Encryption

- Use of Cryptographic Algorithms together with the appropriate Security Keys.

## Key Management & Distribution

- Requirement for a security infrastructure including Certification Authorities.

## Legal Framework and TRUST

- For example: Digital Signatures need to be acceptable in a Court of Law.



**It is a complex Mathematical Formula**

**The name derives from that of a 9th century Persian mathematician**

**Algorithms provide the “Locks” for Digital Signatures**



## Symmetric Algorithms

- a single *Secret Key* is used for both *encryption* & *decryption*
- sender and recipient must share the same key

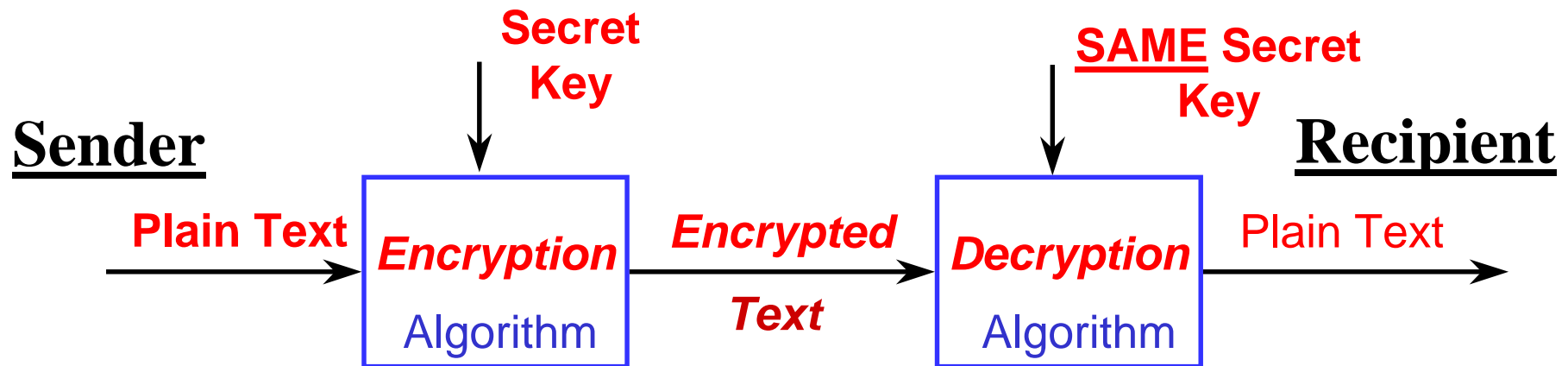
## Asymmetric Algorithms

- a *Key Pair* belongs to an “owner” : *Private & Public Keys*
- one key used to encrypt and the other key to decrypt
- the private key is kept secret; the public key is made widely available

## One-way Hash Algorithms

- used to produce a *Digest* or *Hash*





Used to encrypt data for *secrecy*.

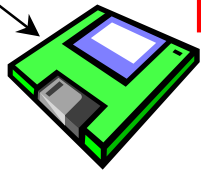
Orders of magnitude faster than asymmetric algorithms.

Normally used with a Session or Message Key,  
a one time only Symmetric Key generated especially for  
the purpose.

Every Key Pair  
belongs to an “Owner”



**Public Key - Widely Distributed**

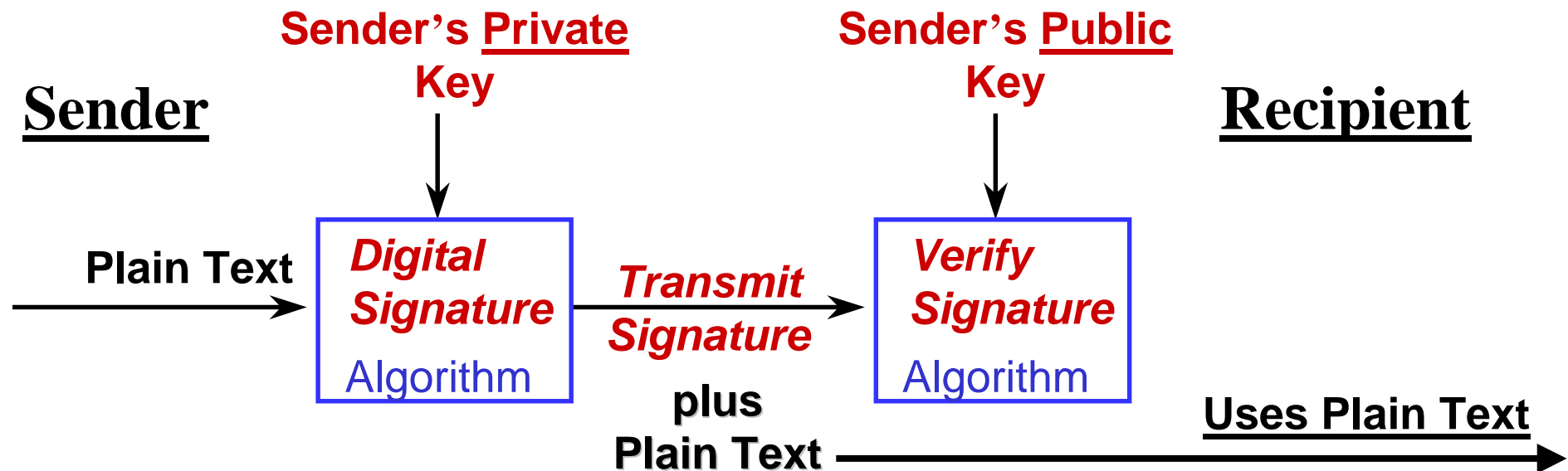


**Private Key - Owner Responsible  
for Safeguarding**

**Private Key is usually kept on a Diskette  
or on a Smart Card (more secure)**

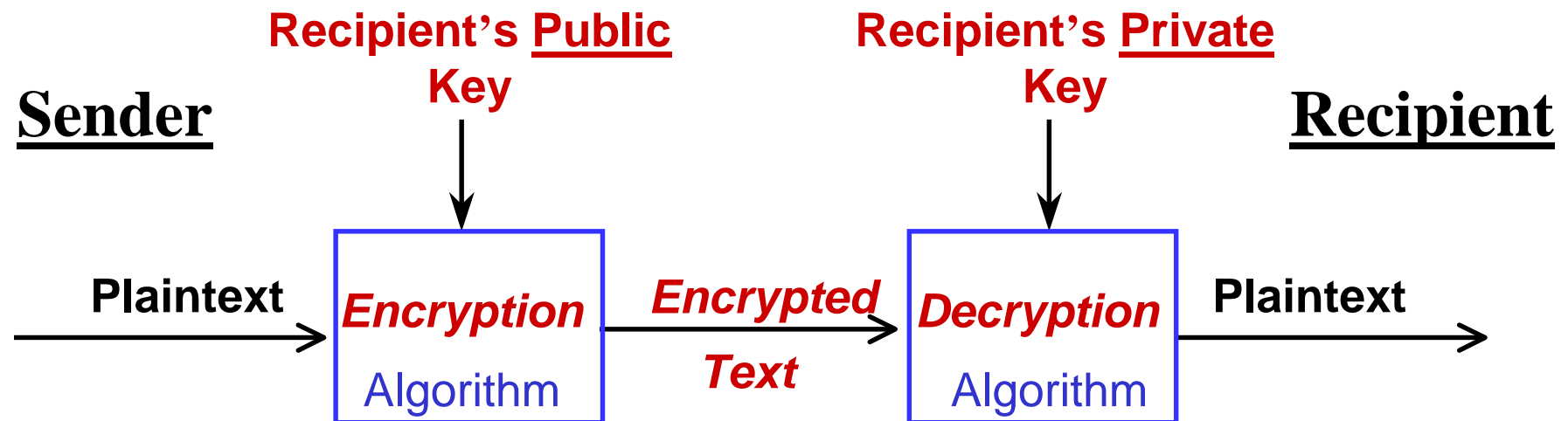
**Protected by a Password or PIN**

## For Digital Signatures using the Sender's key pair



**Allows anyone to check origin and integrity of the message or data**

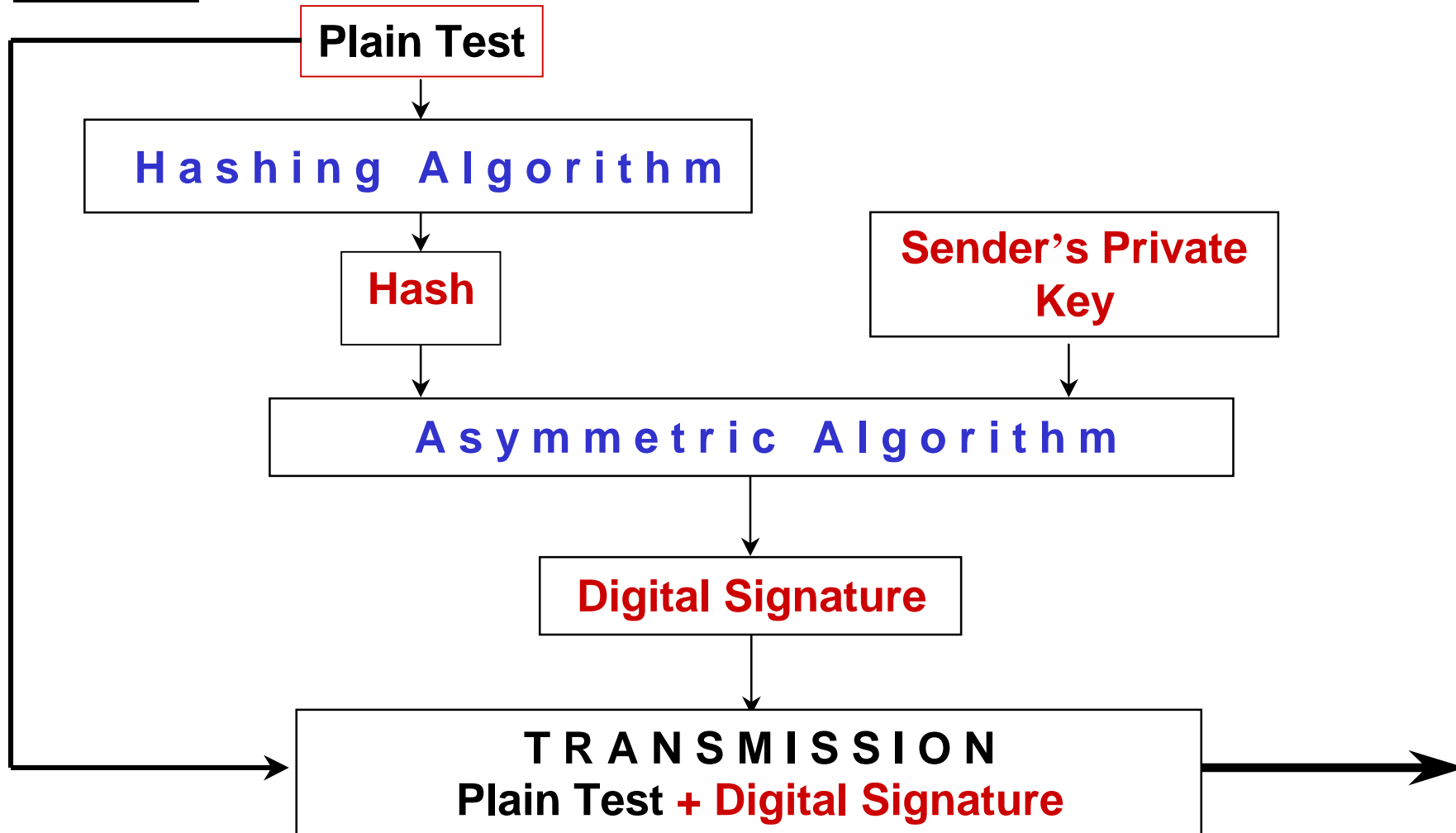
**For Encryption**  
**using the Recipient's key pair**



Keys are used in reverse to send a secret message  
or secret data to the key owner,

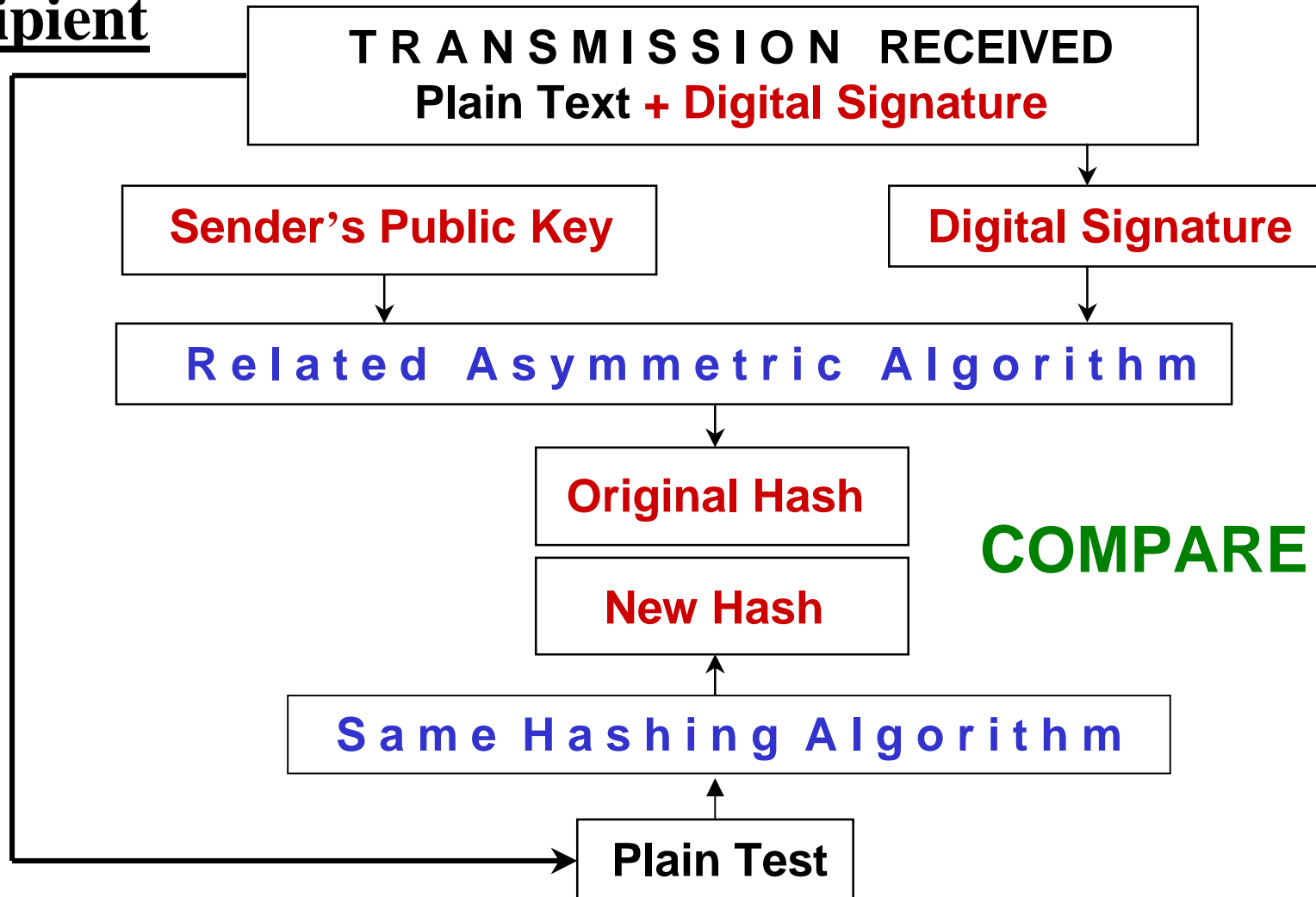
**but the encryption process may be slow.**

## Sender



# VERIFYING A SIGNATURE

## Recipient



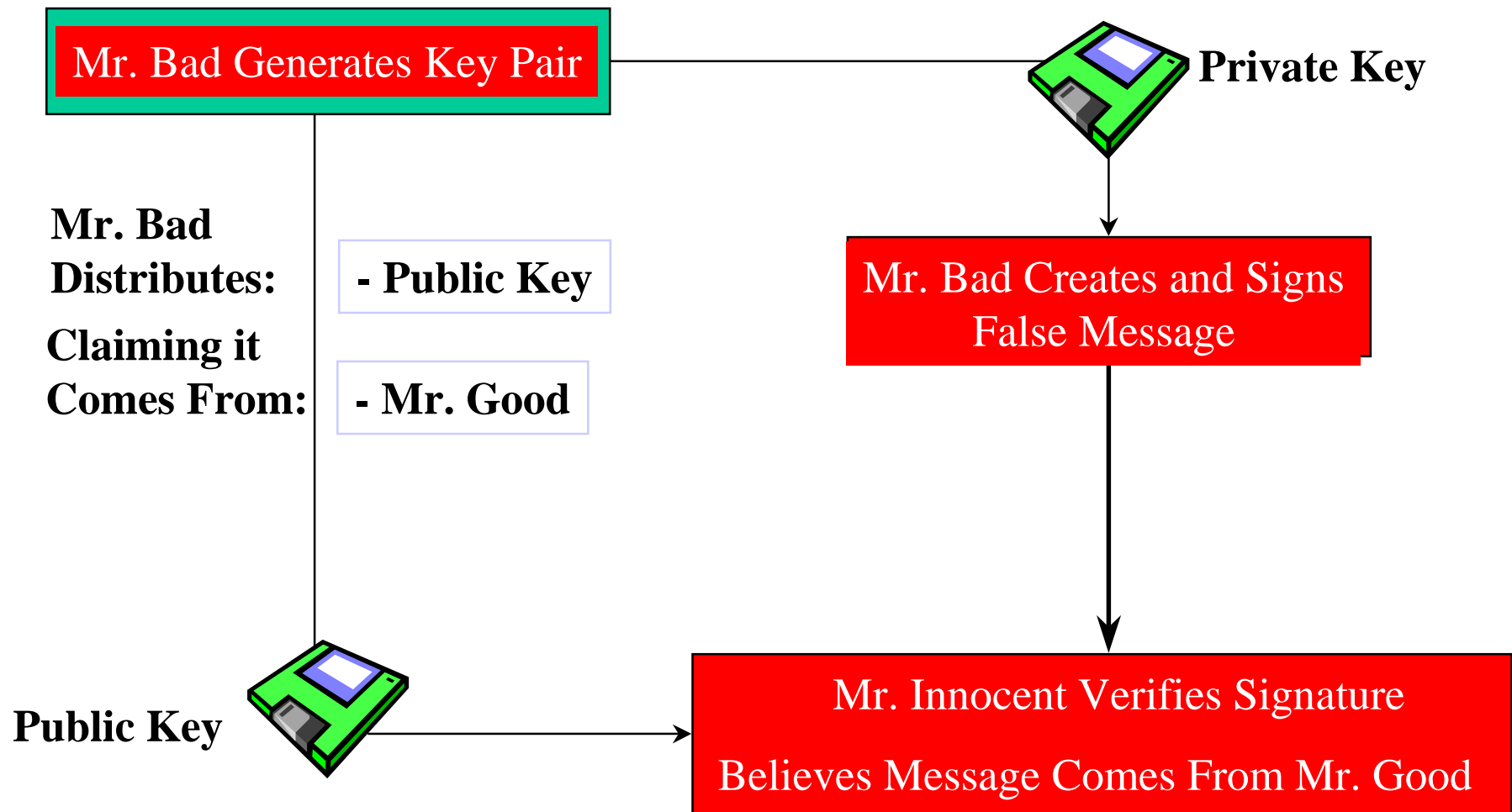
- **Authentication of Origin**
- **Integrity of Data**
- **Non-Repudiation**

**Could use the Asymmetric algorithm, that is the Public/Private Keys, but encryption may take too long.**

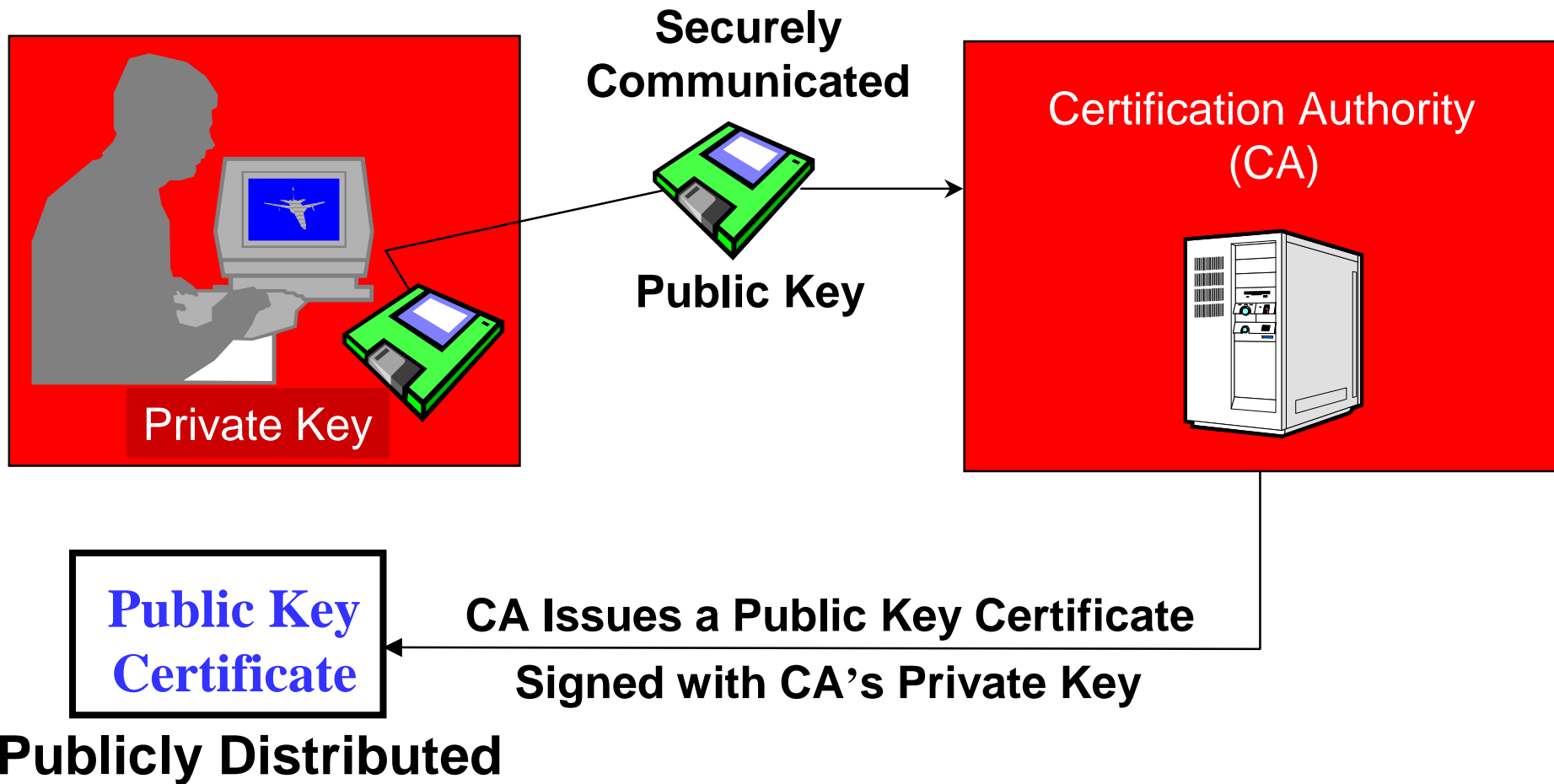
**Better to create a one-time Secret Symmetric Key for encryption (a “Session Key”) and complete the encryption using that Session Key.**

**Then send the encrypted message together with the Session Key, which is itself encrypted using the Public/Private Key Asymmetric algorithm.**





## User Generates Key Pair



**TRUST in Digital Signatures is provided by the Public Key Certificates issued by Certification Authorities (CAs).**

**BUT –**

**How do we know our own CA is to be Trusted?**

**What Trust can we place in Certificates issued by other CAs, both Domestic and International?**

**A number of Trust / Accreditation / Cross Certification models exist, but none is truly Universal, resulting in major problems in the use of Digital Signatures in an Open environment.**



**European Electronic Signature Standardization Initiative  
(EESSI)**

**<http://www.ict.etsi.org/eessi/EESSI-homepage.htm>**

**THE GOAL –**

**To provide a set of standards for Electronic Signatures  
and to harmonize specifications at an International level.**

**THE ALTERNATIVE –**

**An environment governed by proprietary solutions,  
creating a great many isolated islands, lack of flexibility,  
and added costs for users and service providers.**





**An industry-led self regulated initiative for the Approval of Trust Services**

**An independent not-for-profit organization incorporating a broad range of stakeholders who include:**

***Service Providers, Technology Companies,  
Governments and Users***

**<http://www.tScheme.org>**

With Acknowledgement to tScheme



**APACS**

**Barclays**

**Royal Bank of Scotland**

**ViaCode**

**British Chambers of Commerce**

**BT Ignite**

**Baltimore**

**CSSA**

**ICL**

**CBI**

**Hitachi**

**Notaries for eCommerce**

**Notus Key**

**Microsoft**

**Nexus TSP**

**Equifax Secure**

**Dun & Bradstreet**

**e-Centre**

**FEI**

**IBM**

**Lloyds TSB**

**DTI**

**Office of the e-envoy**

**DeLaRue Interclear**

**Vodafone**

With Acknowledgement to tScheme



**tScheme defines the Approval Profiles required for Certification Authorities and other Trust Service Providers in order that they may be issued with a **Grant of Approval**.**

**It has responsibility for the Granting of Approvals.**

**It Reviews, Renews and Revocates Approvals.**

**It handles Complaints (Mediation / Redress).**

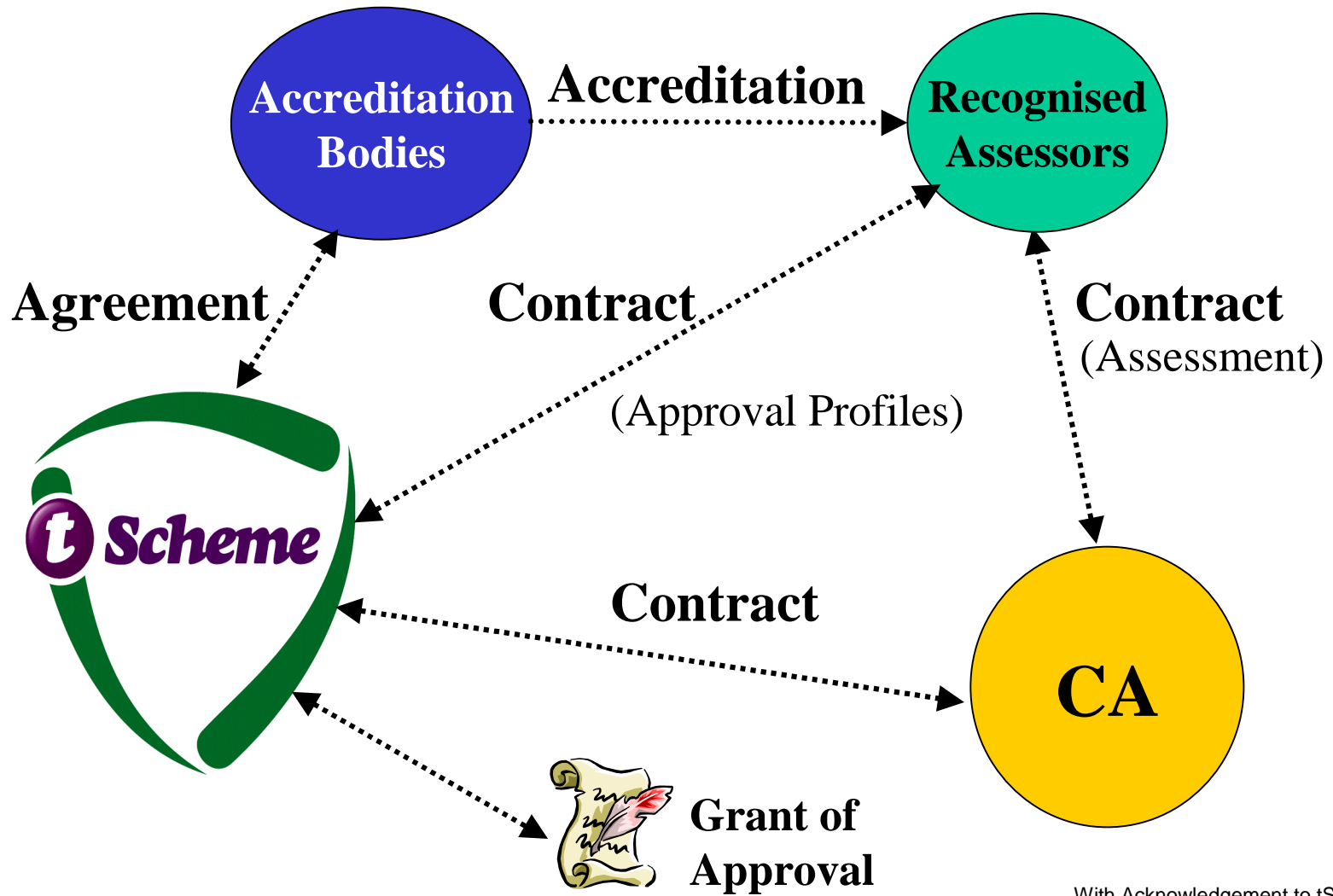
**It Promotes Approved Trust Services.**

**It does not itself actually provide Trust Services.**

With Acknowledgement to tScheme



# THE APPROVAL PROCESS



## WHAT DOES tSCHEME APPROVAL MEAN?

- The Service has been thoroughly evaluated against rigorous criteria by independent experts.
- The Service Provider has agreed to keep to these criteria.
- The Service Provider subscribes to the tScheme Code of Conduct.
- The Service Provider has agreed to act promptly and fairly to remedy faults.
- **IT OFFERS A HIGH DEGREE OF TRUST IN THE SERVICE PROVIDER**

With Acknowledgement to tScheme



# THANK YOU

Compiled and Presented by

**John Daly**  
**Senior Consultant**  
**Critical Path Asia Pacific**

**john.daly@cp.net**

**jad@pacific.net.hk**

**www.cp.net**

The opinions expressed herein are those of the Presenter  
and do not necessarily represent the views Critical Path

