Security & Wireless

Ing. Mirko Tedaldi
CryptoNet S.p.A.
mirko.tedaldi@cryptonet.it

CRYPTONET
sicurezza, reti, sistemi

Overview

- Introduction: who is CryptoNet
- Wireless scenario
- Wireless Virtual Private Network
- Wireless LAN
- M-commerce and Wireless Public Key Infrastructure

CryptoNet: who we are

- The only Italian Company 100% devoted to security (infosec as the only business area, from corporate security policy design to router secure configurations);
- Committed to enable Customer INNOVATION as a way to gain Competitive Advantage
- **1995**: first mass market Crypto SC in Italy; first WWW-based Information System over the Internet in Italy
- **1996**: first Corporate Internet-connection security CERTIFICATION in Italy
- **1997**: first secure Internet Home banking in Italy; introduction of first Active RSA SC in Italy
- **1998**: very large "BNL Group security" contract; the first Ipsec WW network in Europe (Luxottica); first IPSEC demo with CISCO in Europe (TIM).
- **1999**: the two largest Ipsec VPNs in the world with CISCO (1000 routers, OMNITEL 2000, 20.000, RUPA...); the first on-line trading with digi sig and timestamping
- **2000**: the largest SSO and digi sig integration for SAP (40.000 seats) in Europe, implemented in 12 Weeks from contract signature;
- Customers list: FIAT, ENEL, ENI, Pirelli, SIA, CSELT, SSGRR, BNL, Magneti Marelli, Urmet, ABB, Luxottica, Omnitel, SOGEI/Ministero delle Finanze, RUPA, Ministero del Tesoro, WIND … … … ;
- Good experience in the technical, regulatory and business-drivers fields.

CRYPTONET
sicurezza, reti, sistemi

Le tecnologie

APPLICATION	Authorization	VPD		
USER	Users/Group	SSO	Authentication	Token e SmartCard
DATA	Encryption	Hashing	Digital Signature	
SYSTEM	Auditing	Virus Prevention	Intrusion Detection	
NETWORK	Firewall	VPN	Router	Virtual LAN

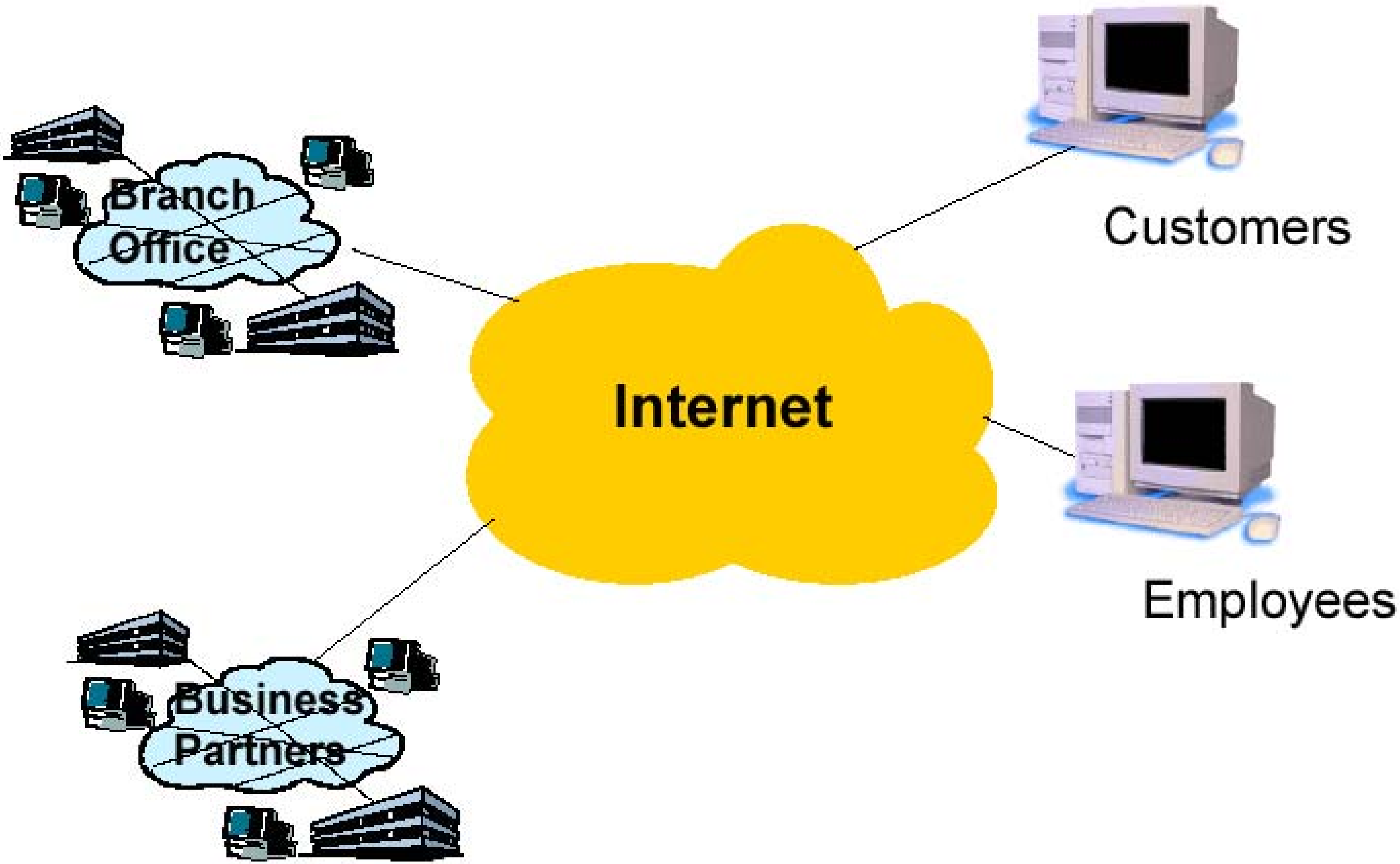
Risk Assessment

Risk Analysis

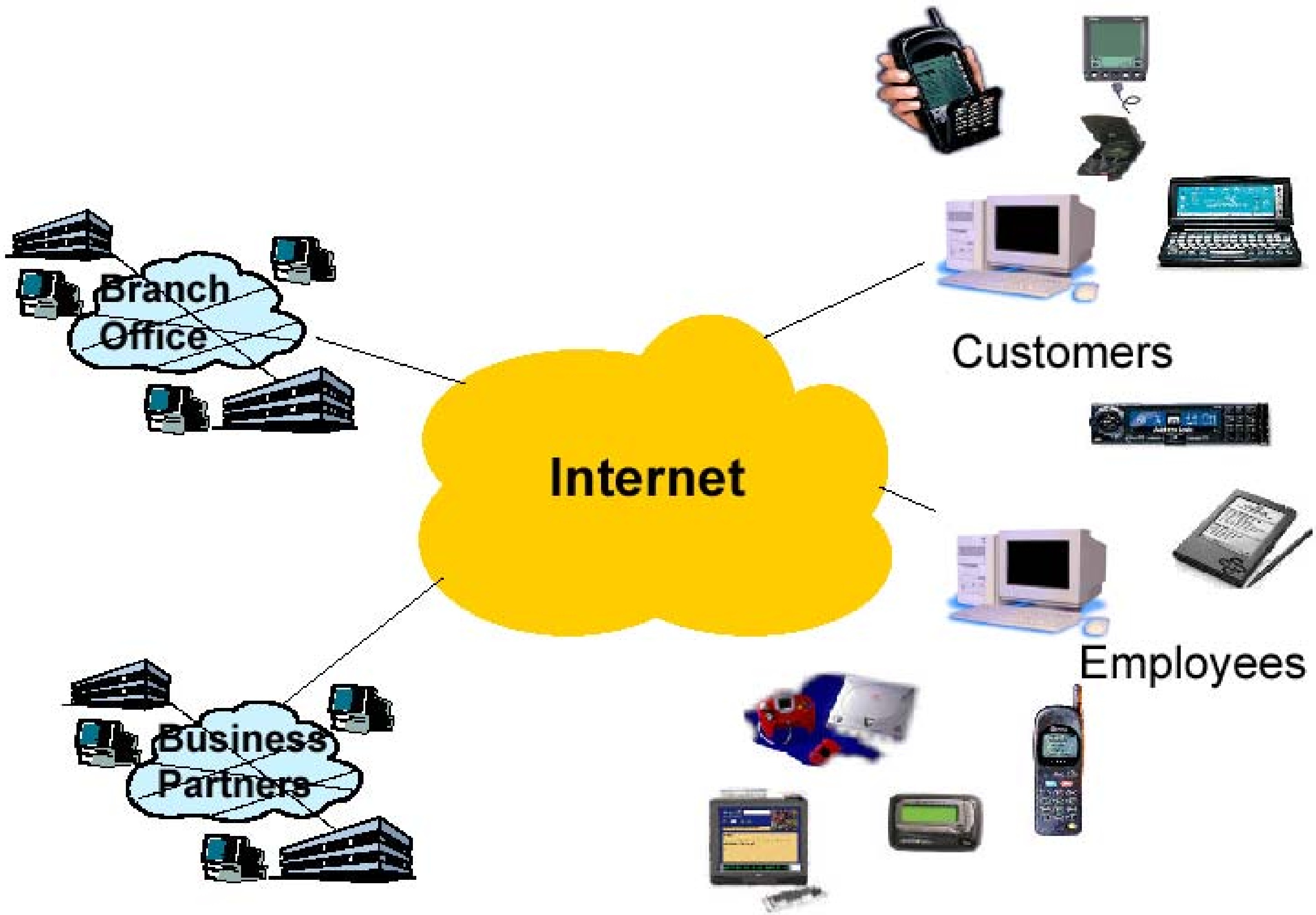
CC e ITSEC

CRYPTONET
sicurezza, reti, sistemi

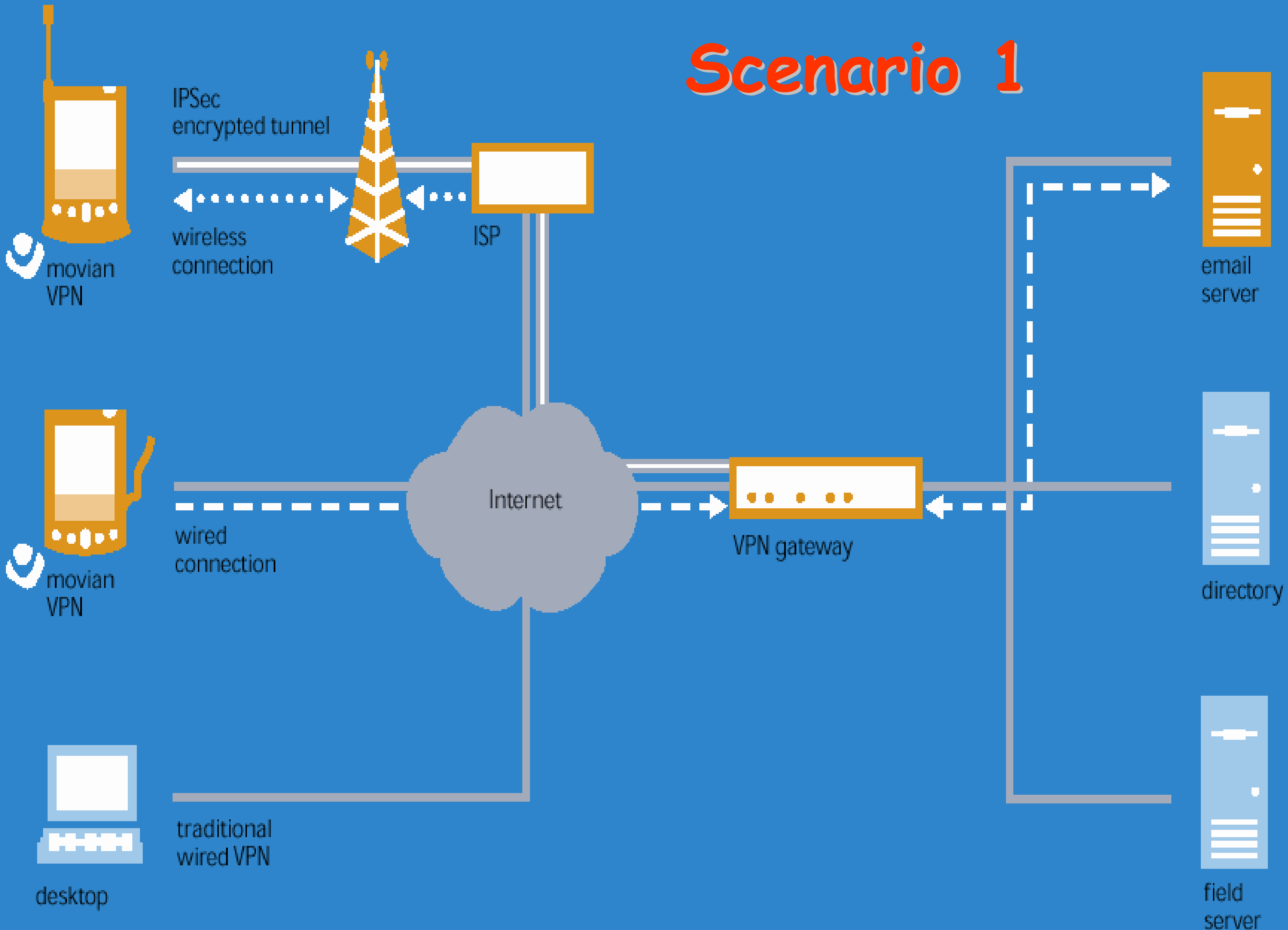
Virtual Enterprise today…



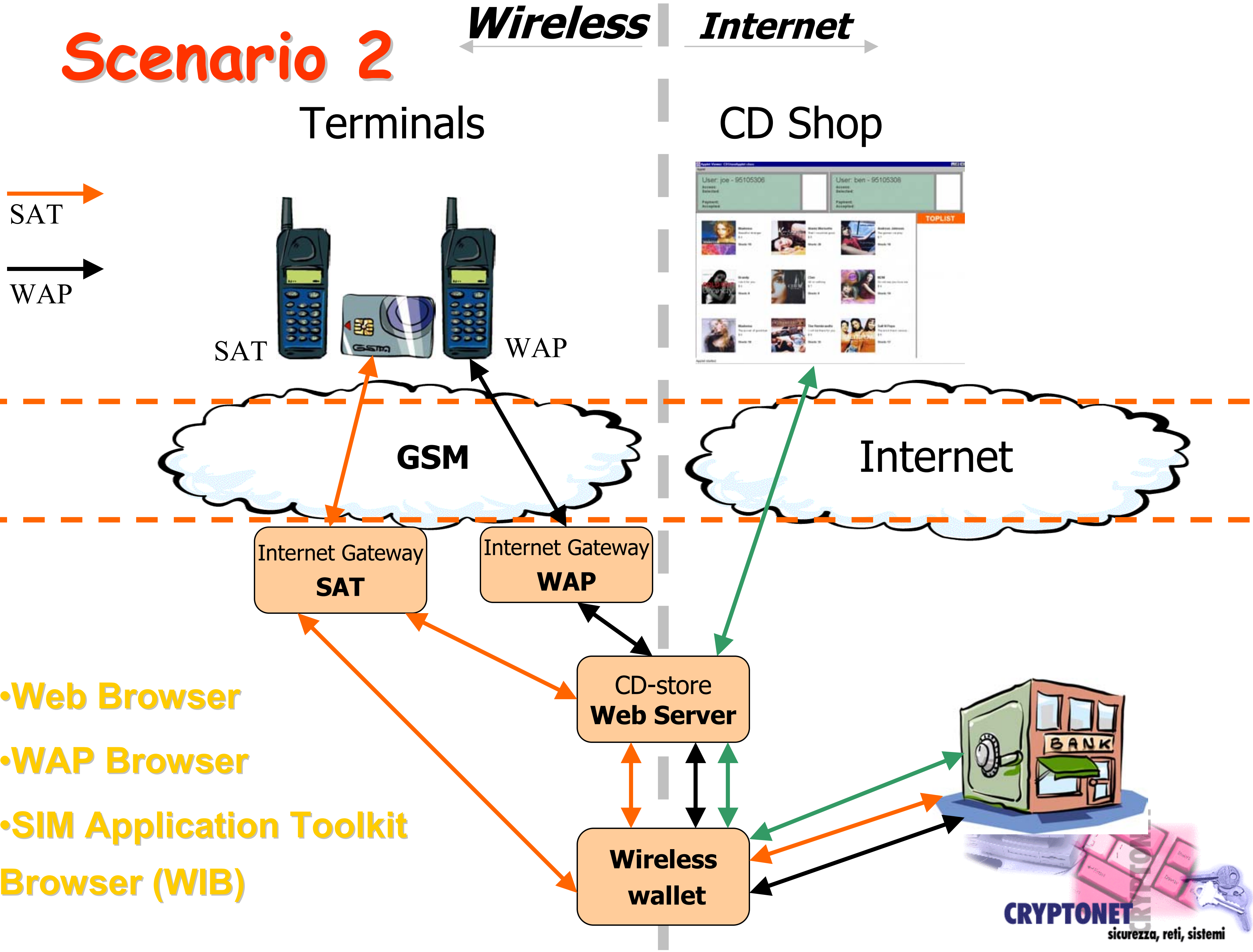
… add devices


Branch Office
Internet
Customers
Employees
Business Partners

Scenario 1


IPSec
encrypted tunnel
wireless
connection
ISP
movian
VPN
email
server
Internet
VPN gateway
wired
connection
movian
VPN
directory
traditional
wired VPN
desktop
field
server

Scenario 2

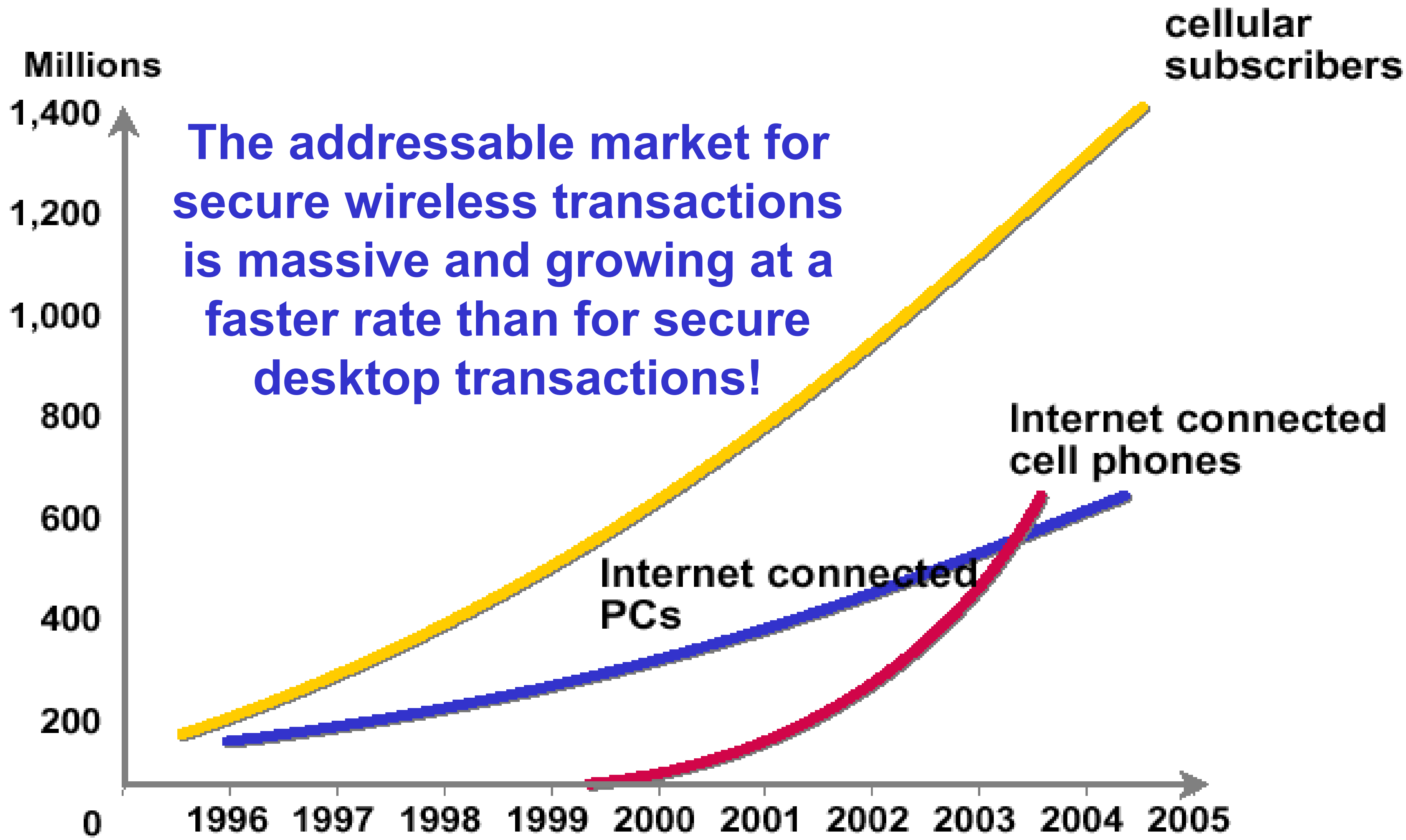


- Web Browser
- WAP Browser
- SIM Application Toolkit Browser (WIB)

Security services in Wireline/Wireless

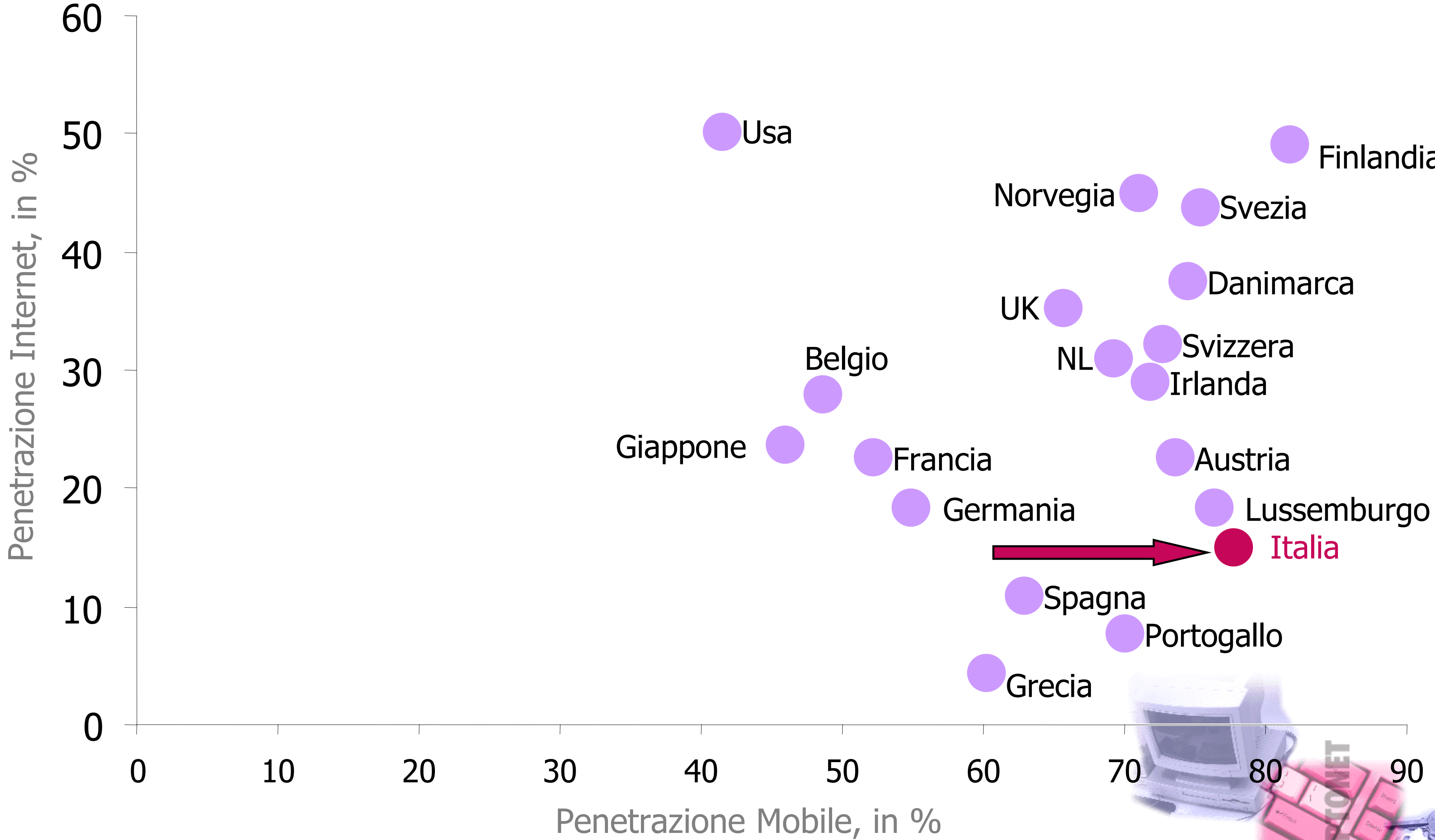
- **Confidentiality**
  - No-one can listen to your communication
- **Integrity**
  - No-one can change the message
- **Server Authentication**
  - You know who you are communicating with
- **Client Authentication**
  - They know they are communicating with you
- **Non-repudiation**
  - An agreement is not disputable

Internet Users



Source: WAP forum

Mobile users vs InterNet Users



Fonte: Smau/EITO 2001

Wireless Data

•Data that is bursty and always-on, needs a packet infrastructure (vs. modem pool arrangement)

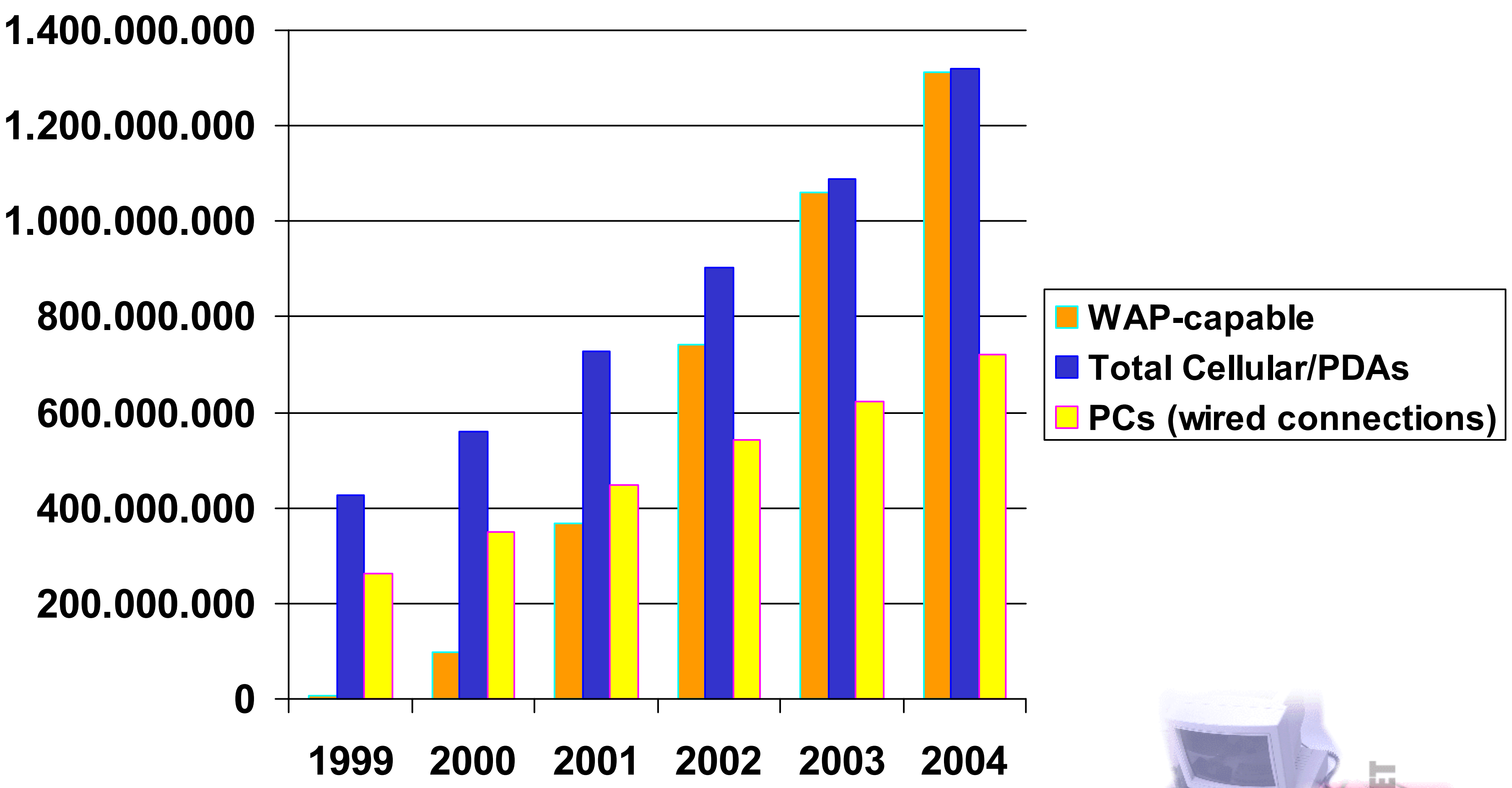
2G	9.6 Kbps
2.5G	‘up to’ 100 Kbps
3G	2 Mbps

Today, circuit switched

2001, packet switched

2003, packet switched

Market is huge!



Source: IDC, 2000

Lo scenario del Mobile E-commerce in Europa Occidentale

- 250 milioni di utenti di telefonia mobile nel 2000 (+60% a fine 1999)
- 400 milioni di utenti di telefonia mobile nel 2003
- penetrazione pari al 100% in molti Paesi
- gli utenti di Internet raddoppieranno prima del 2005 rispetto ai 120 milioni del 2000

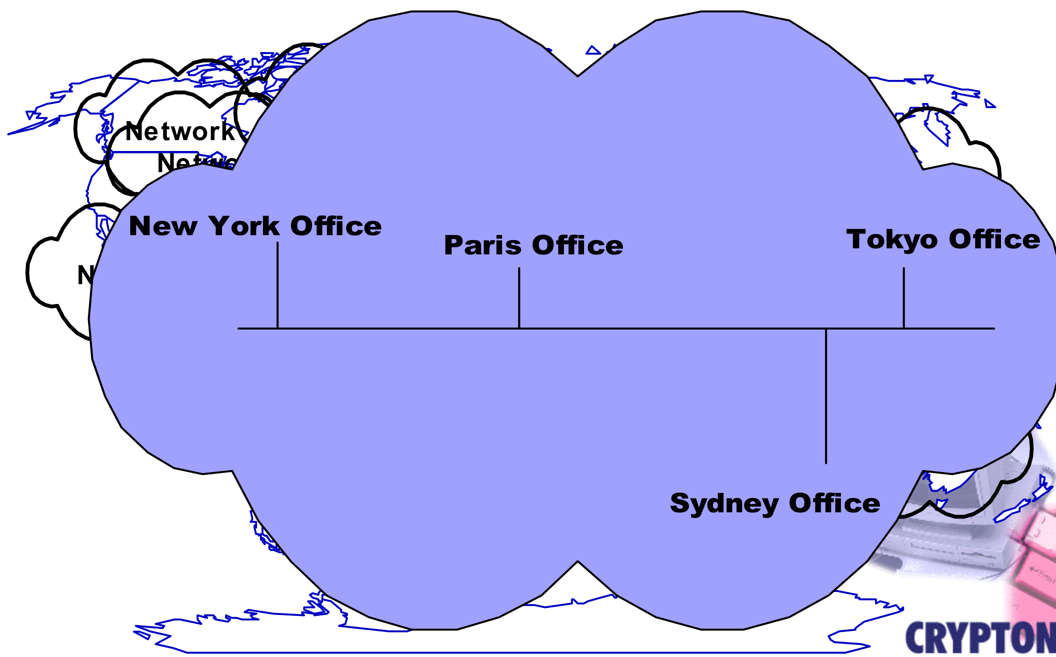
MOBILE E-COMMERCE

- 2001: 24 milioni di utenti
- 2003: 100 milioni di utenti e 38 miliardi di Euro di ricavi
- 2005: 175 milioni di utenti e 86 miliardi di Euro di ricavi

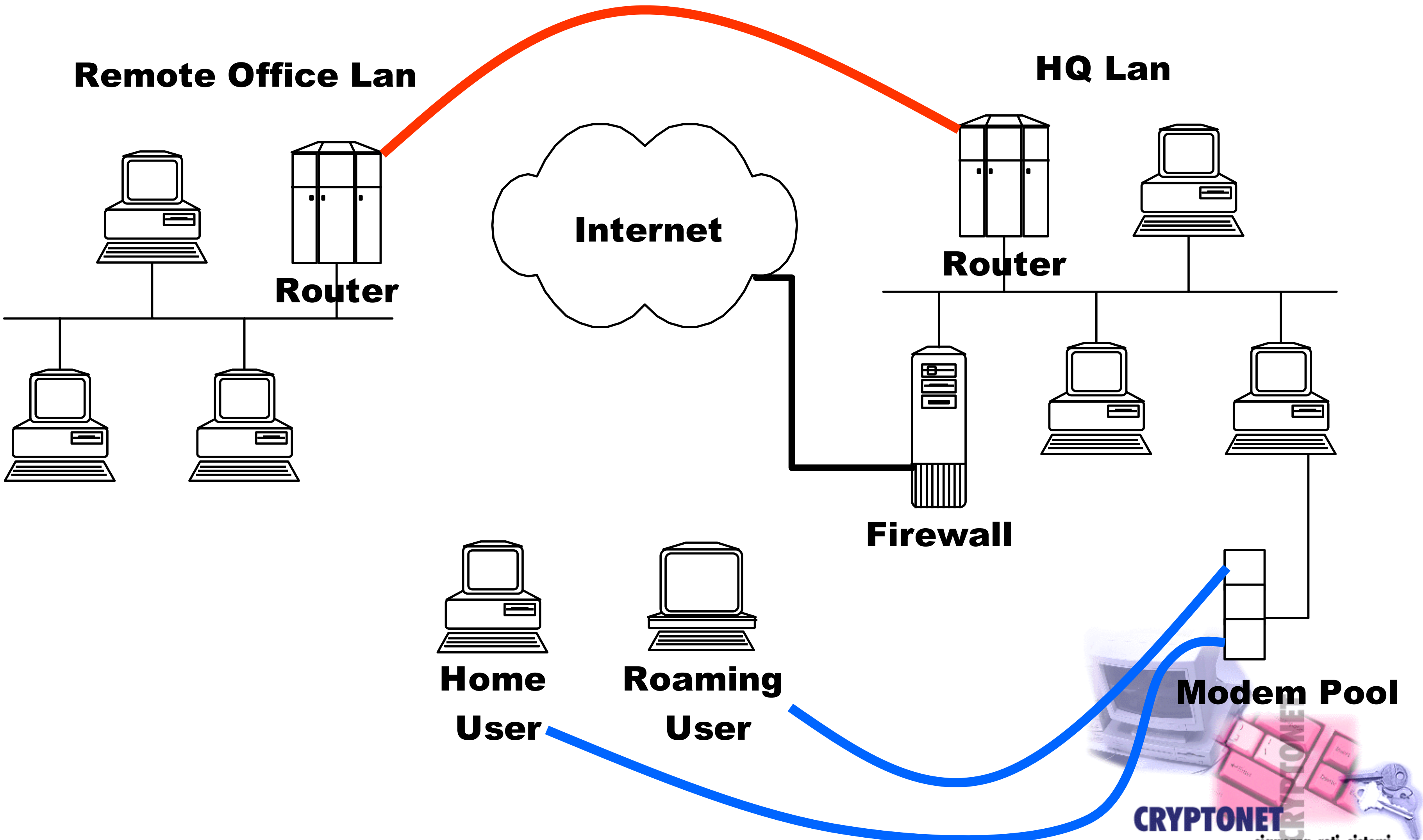
CRYPTONET
sicurezza, reti, sistemi

What is a VPN?

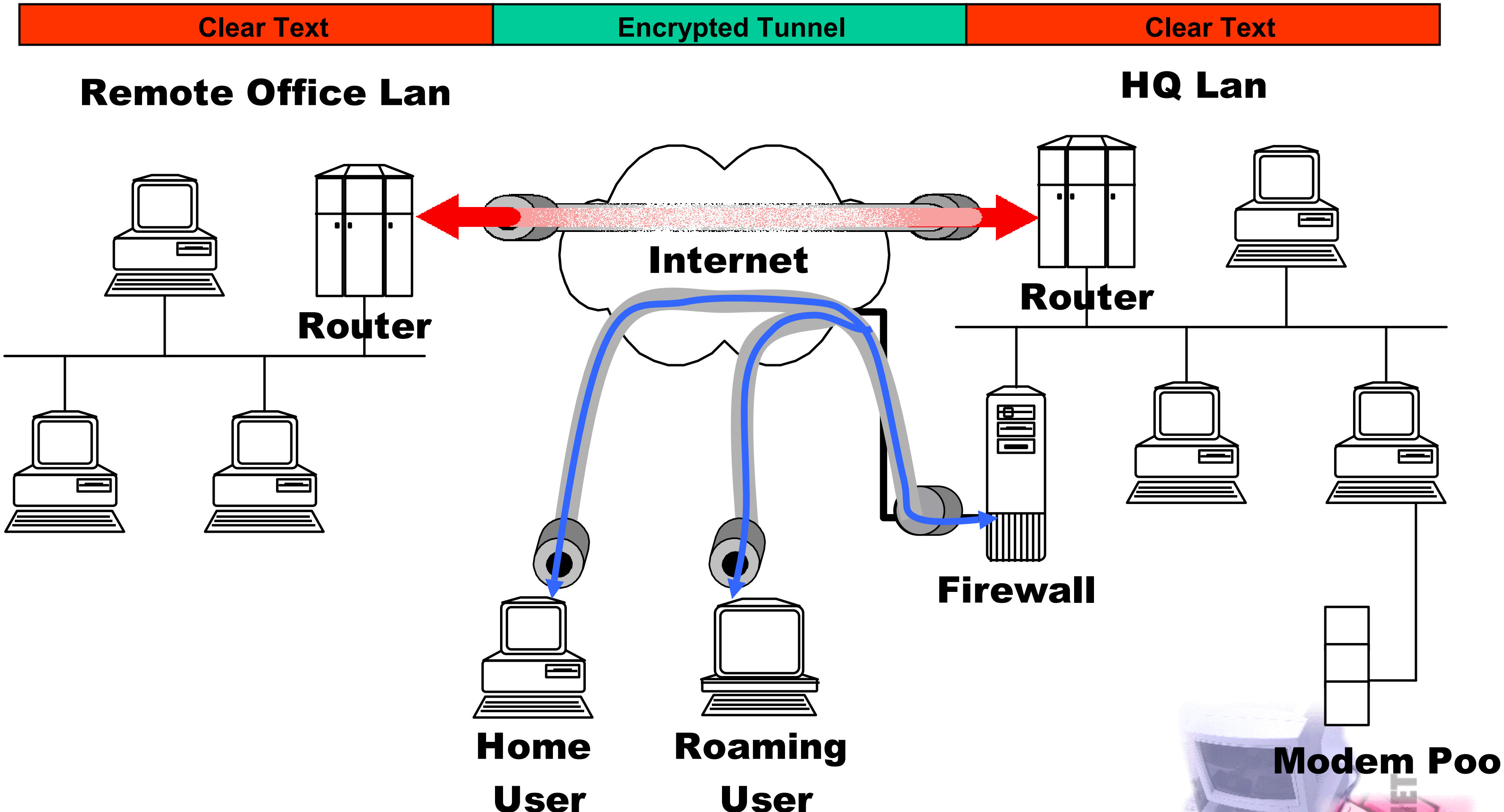
- At its simplest, a VPN (Virtual Private Network) is a network built on top of the services of another network
  - often VPNs are built on the public Internet, but not always



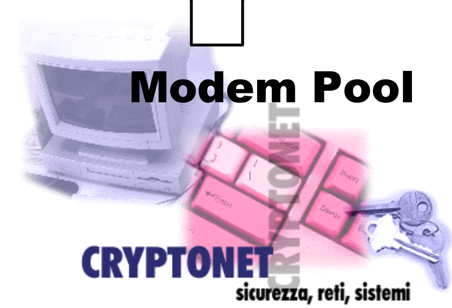
Prevailing Methods



VPN Methods

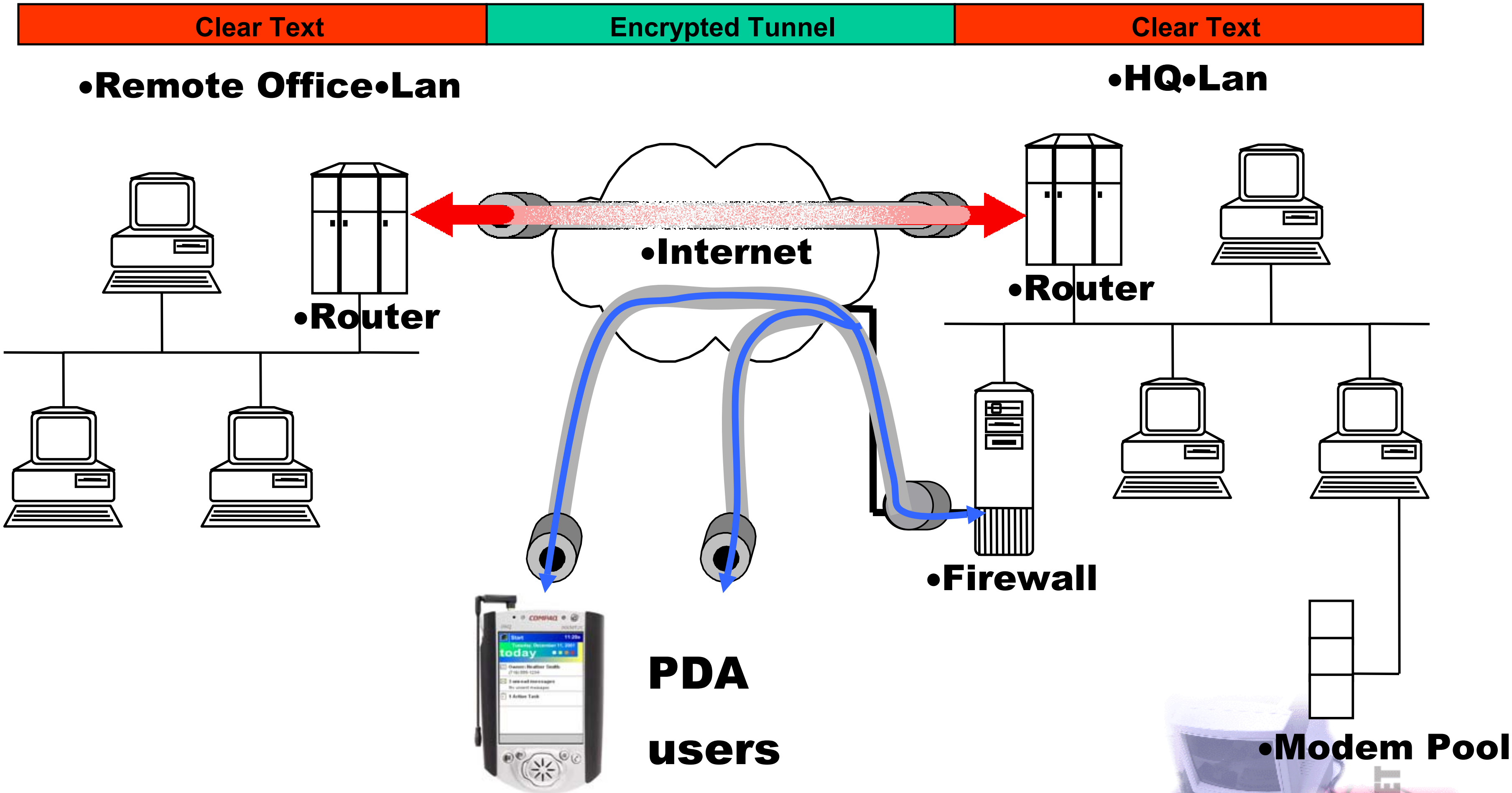


Clear Text
Encrypted Tunnel
Clear Text
Remote Office Lan
HQ Lan
Router
Internet
Router
Firewall
Home User
Roaming User
Modem Pool



CRYPTONET
sicurezza, reti, sistemi

Wireless VPN



CRYPTONET
sicurezza, reti, sistemi

PDA: iPAQ Pocket PC

Processor	Intel StrongARM 32-bit RISC 206MHz
RAM	32MB – 64MB
ROM	16MB – 32MB (flash)
O.S.	MS Pocket PC 2000/2002 (MS Win CE 3.0)
Display	TFT LCD 240x320 64K color
Ports	USB, serial, Infrared
Connectivity	Modem 56K Ethernet 100MBps *(Q4/01)*
Memory card slot	Up to 128MB (or 1GB removable HD)
Wireless pack	GSM/GPRS *(Q1/02)* Bluetooth *(Q4/01)* IEEE 802.11

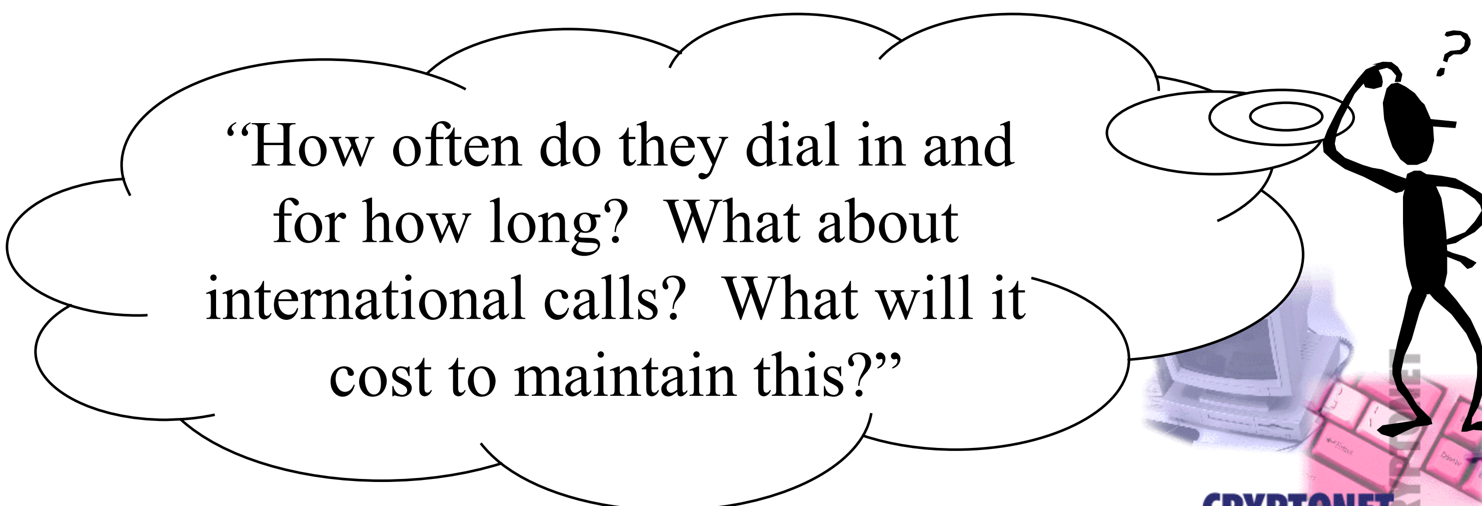
Uses for VPNs

- **Intranet VPN:**
  - between a central corporate and branch offices
- **Remote VPN:**
  - between a central corporate and individual remote users
- **Extranet VPN:**
  - between an enterprise and its business partners, suppliers and customers

Remote VPN and Extranet VPN include not only mobile devices like laptops, but wireless handheld devices like PDAs and smart phone.

Business Reasons for VPNs

- Increased business being done over Internet
- Secures communications at network layer (IP) across all applications (including legacy apps)
- Cost effective for remote access: compare to a modem pool and long distance charges



The Nature of Secure VPNs

- The classic problems
  - **authentication**
  - **integrity**
  - **confidentiality**

"Which devices do I trust? Which client machines do I trust? Is anyone able to monitor my session? Is anyone able to hijack my session?"

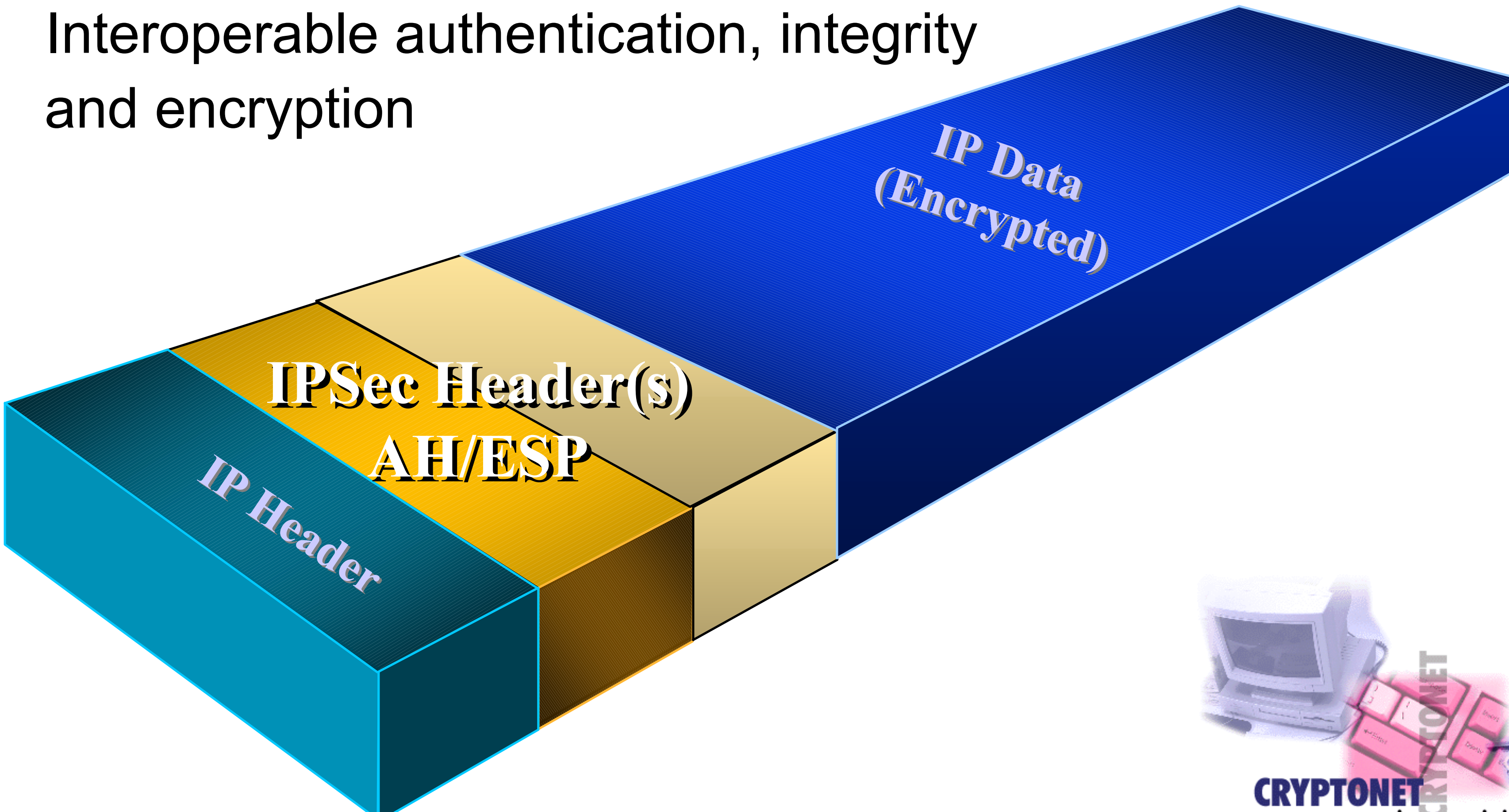
Authentication in IPSec

- **Pre-shared keys**
  – Single key or passphrase per peer
  – Still results in huge numbers of keys in meshed networks

- **Digital signature and certificates (PKI)**
  – Third Party Trust minimizes the number of keys required for strong authentication

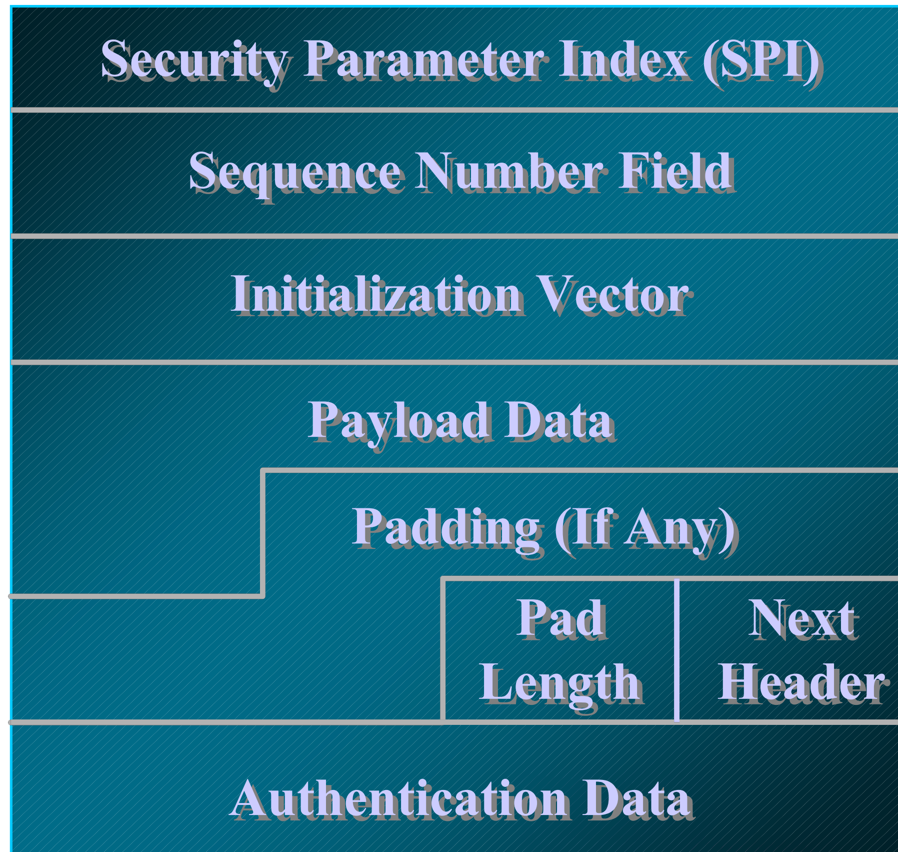
An outline of IPSec

- *"The goal of the IPSec architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments."* (IETF-RFC2401)
- Interoperable authentication, integrity and encryption



Encapsulating Security Payload Header (ESP)

- ESP header is prepended to IP datagram
- Confidentiality through encryption of IP datagram
- Integrity through keyed hash function

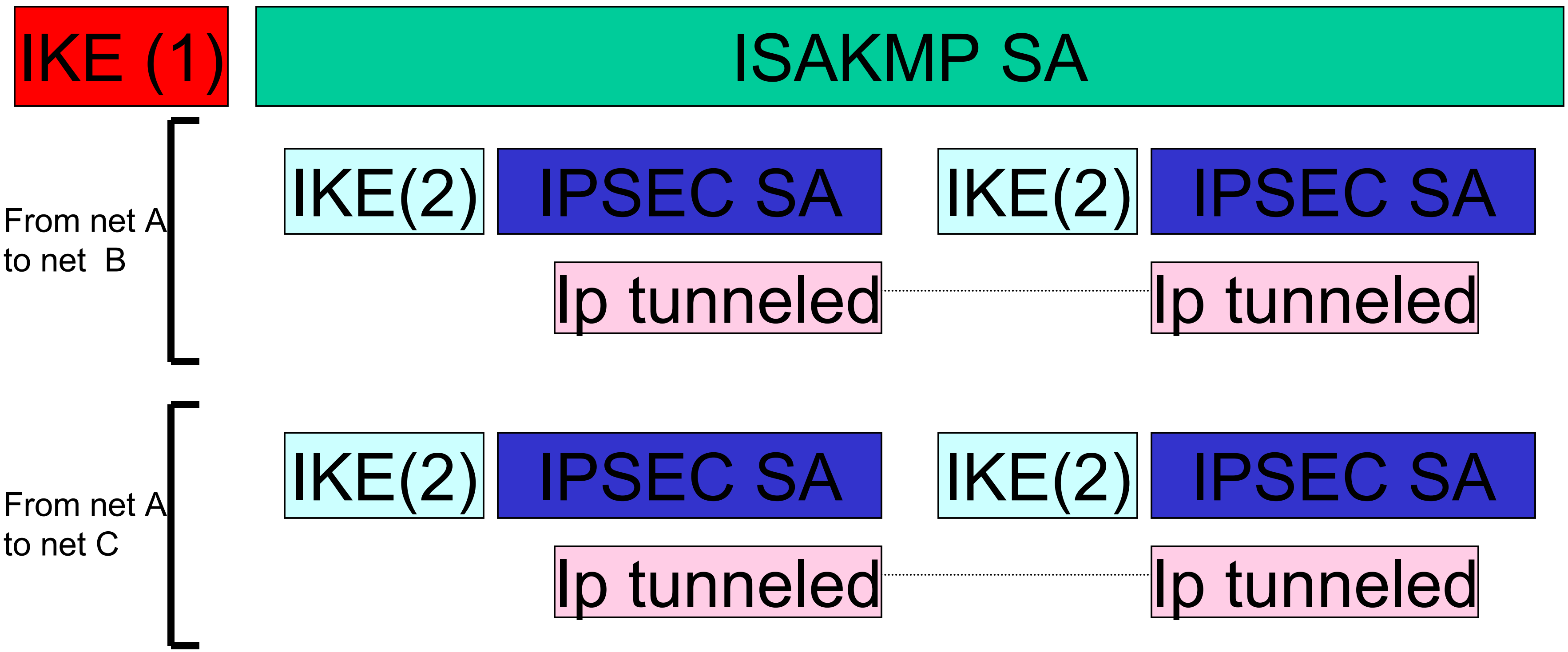


Authentication Header (AH)

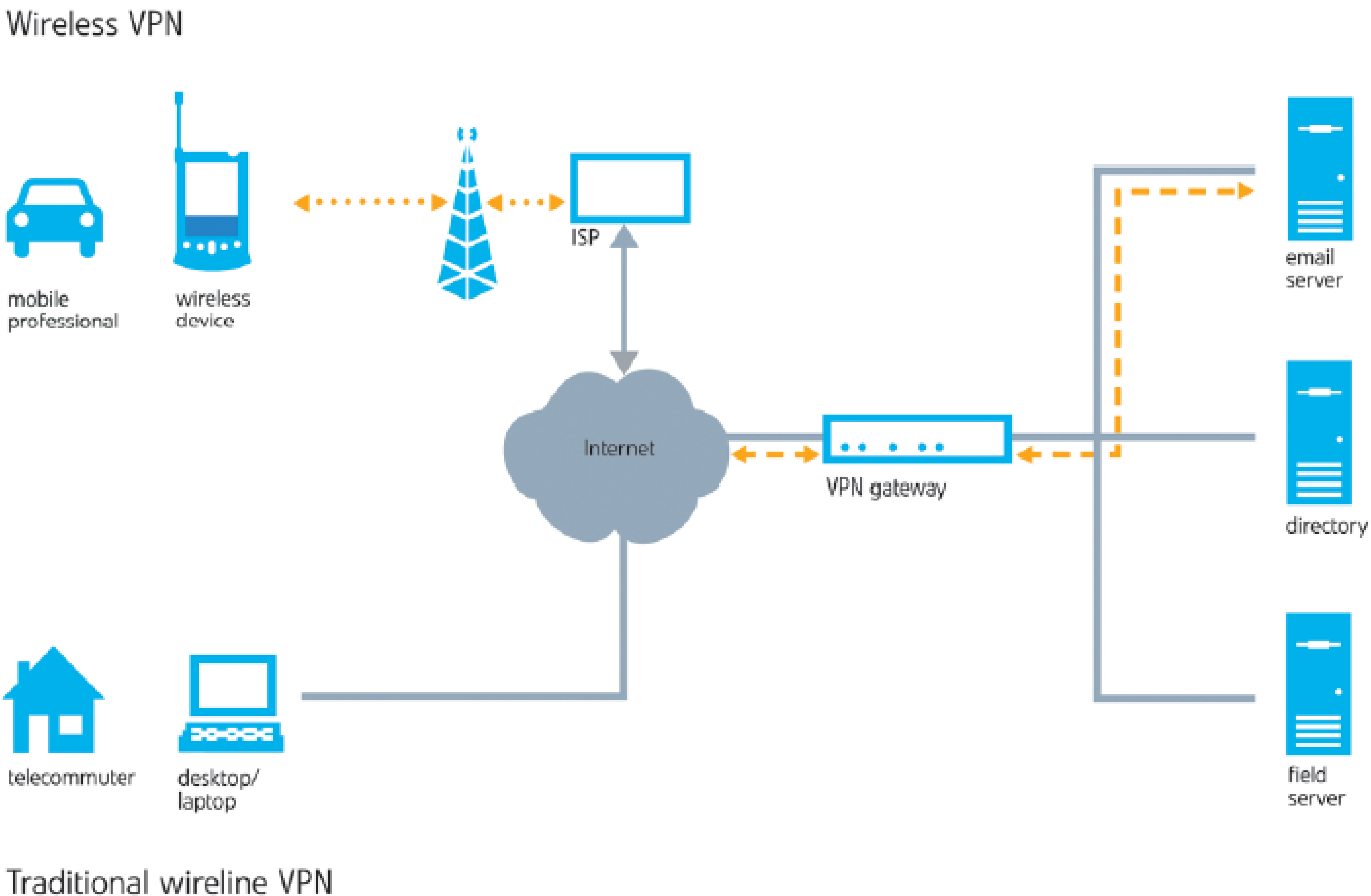
- AH header is prepended to IP datagram or to upper-layer protocol
- IP datagram, part of AH header, and message itself are authenticated with a keyed hash function

<table>
<tr><td>Next Header</td><td>Payload Length</td><td>RESERVED</td></tr>
<tr><td colspan="3">Security Parameter Index (SPI)</td></tr>
<tr><td colspan="3">Sequence Number Field</td></tr>
<tr><td colspan="3">Authentication Data</td></tr>
</table>

IPSec Sessions



Wireless VPN vs Wireline VPN



Wireless connections

- Dedicated dial-up modem to access an ISP through the telephone network
- Wireless modem to access a local LAN
- Modem with data-capable mobile phone to access the ISP

IEEE 802.11b

•It defines the standard for wireless LAN products that operate at an Ethernet-like data rate of 11 Mbps

•Interoperability of wireless LAN products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA; see http://www.wi-fi.com), which brands compliant products as “Wi-Fi.”

•Security: **access control and privacy** between clients and access points

Security: Wired LANs vs Wireless LANs (1)

Wired LAN

1) Access Control:

it is governed by access to an Ethernet port for that LAN.

⇒ access control for a wired LAN often is viewed in terms of physical access to LAN ports.

2) Privacy:

data transmitted is directed to a particular destination,

⇒ privacy cannot be compromised unless someone uses specialized equipment to intercept transmissions on their way to their destination.

Security: Wired LANs vs Wireless LANs (2)

Wireless LAN

1) Access Control:

transmitted data is broadcast over the air using radio waves

⇒ it can be received by any wireless LAN client in the area served by the data transmitter

2) Privacy:

there is no way to direct a wireless LAN transmission to only one recipient.

Installing a wireless LAN may seem like putting Ethernet ports everywhere

How to secure a Wireless LAN

- **Virtual Private Network**:
  - VPN is independent of any native wireless LAN security schema
  - VPN runs transparently over a wireless LAN (as for wired LAN)

- **Wired Equivalent Privacy (WEP)**:
  - An optional encryption schema stipulated by IEEE 802.11

Wired Equivalent Privacy (WEP)

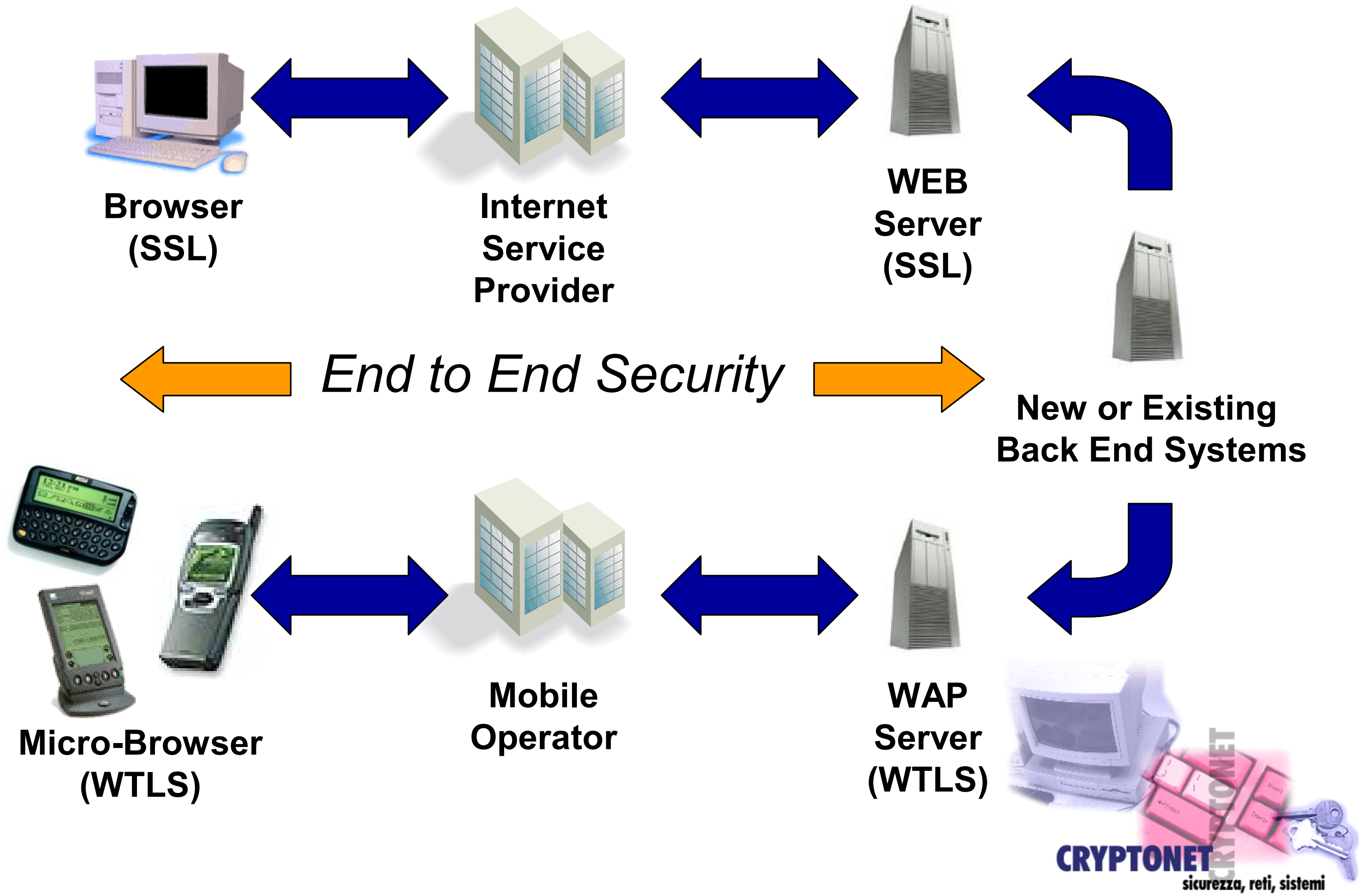
- WEP uses a **symmetric** schema
- Its goals are:
  - Access control
  - Privacy
- Software or hardware implementation of WEP
- Two schema for defining the WEP keys:

  1) Default key schema
  2) Key mapping schema

WEP Authentication

- Two type of authentication methods: open and share key
- The authentication method must be set on each client and the setting should match that of the access point with which the client wants to associate
- **OPEN** (default): the entire authentication process is done in clear-text, and a client can associate with an access point even without supplying the correct WEP key.
- **SHARED KEY**: the access point sends the client a challenge text packet that the client must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the access point.

WEB / WAP Parallels



Security services in WAP

- **Confidentiality**
  - WTLS bulk encryption between WAP Client and WAP GW
- **Integrity**
  - WTLS HMAC construct
- **WAP Gateway Authentication**
  - WTLS Class 2

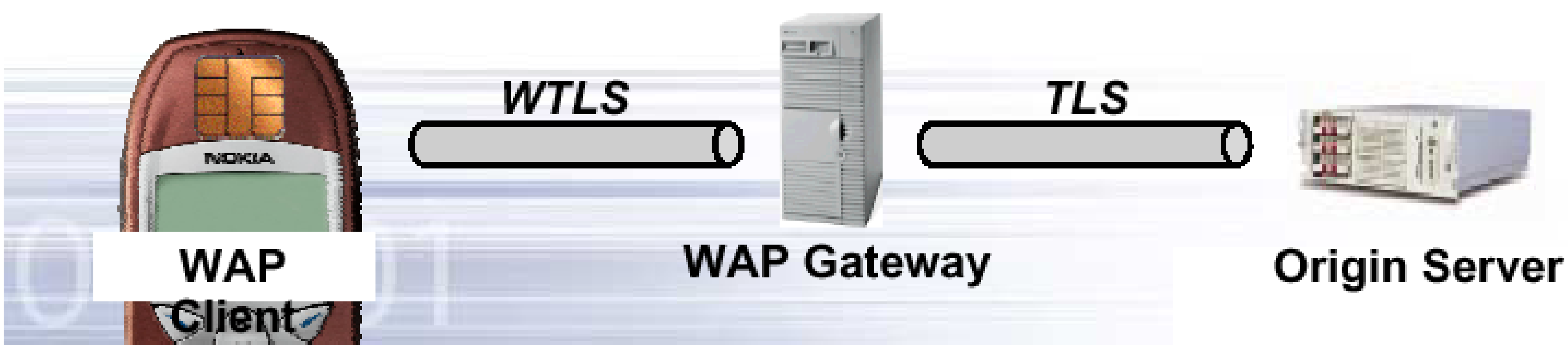
Server certificates

WAP 1.1

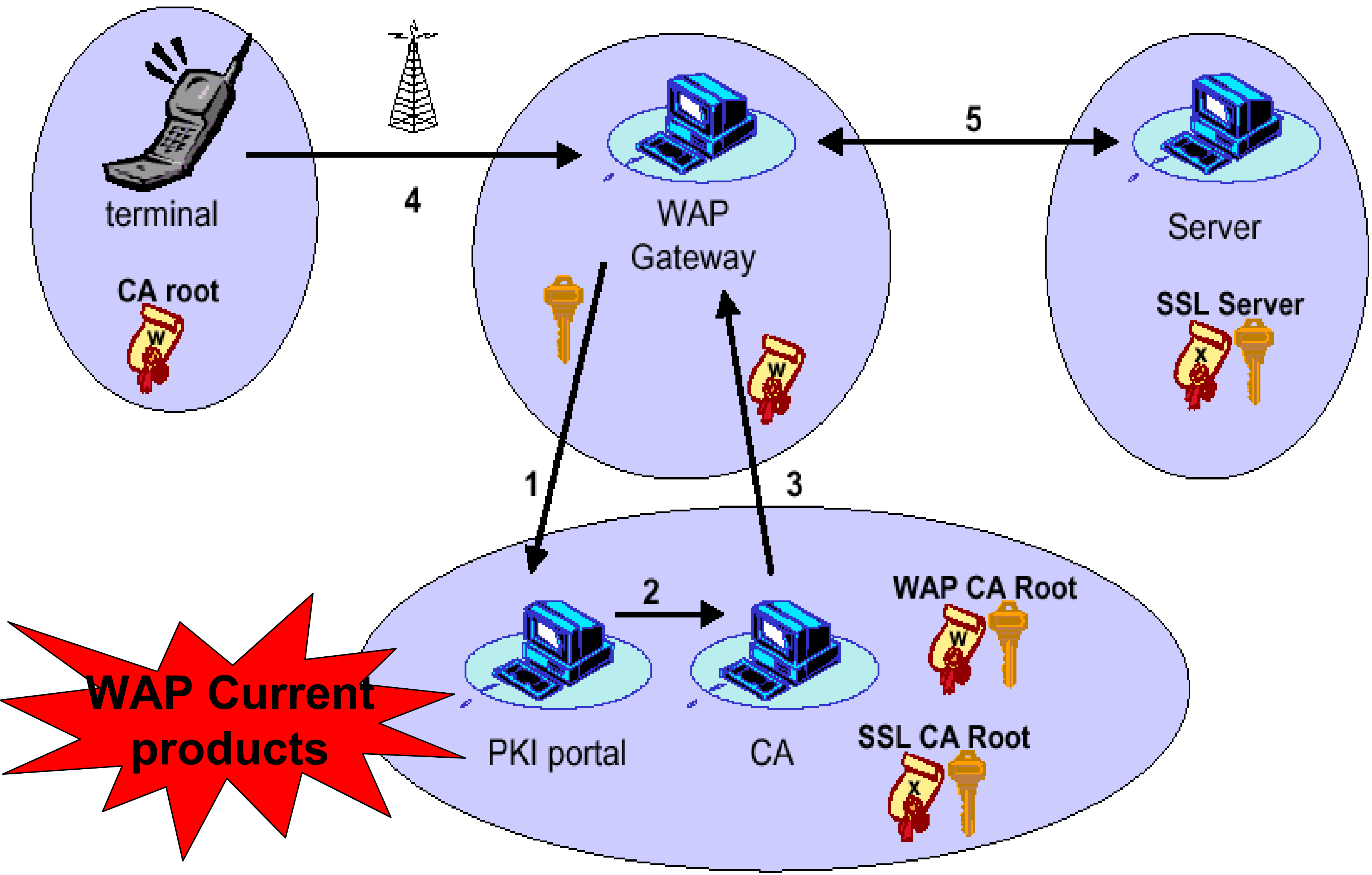
WAP 1.2

- **WAP Client Authentication**
  - WTLS Class 3
- **Non-repudiation**
  - WMLScript CryptoLibrary signText() digital signatu

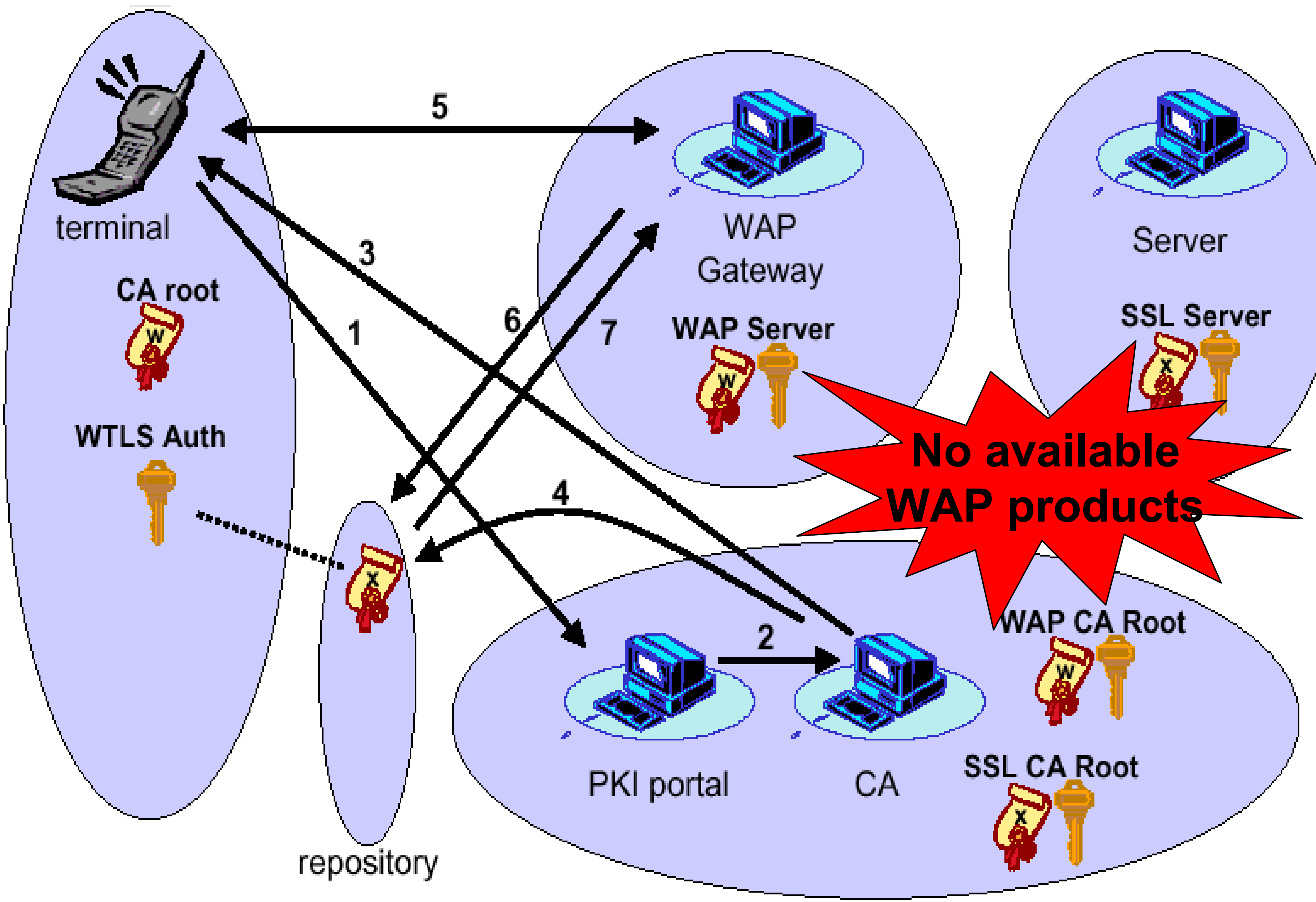
Client certificates



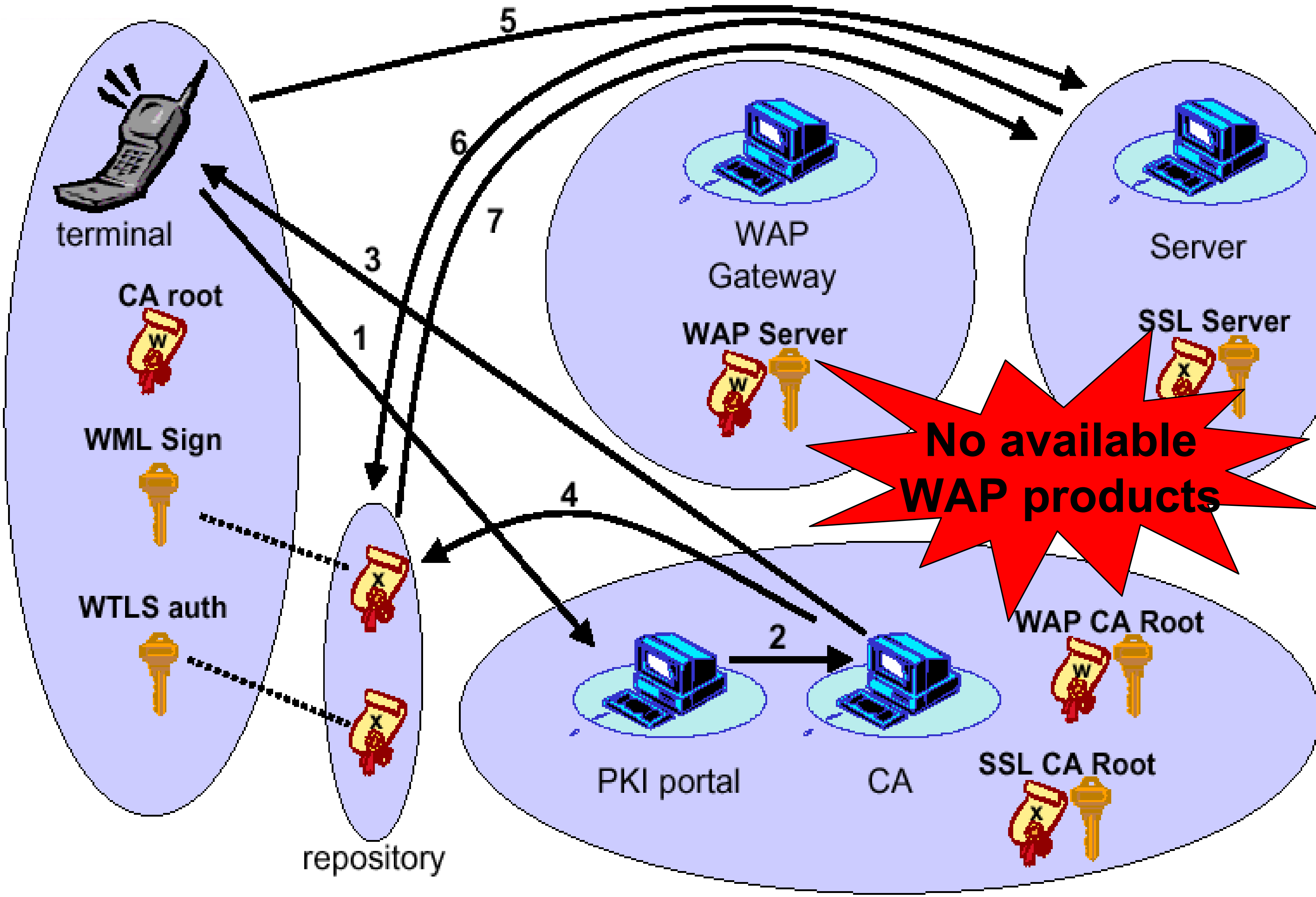
Gateway Authentication



Client (phone) authentication



Digital Signature



Deficiencies of WAP (1)

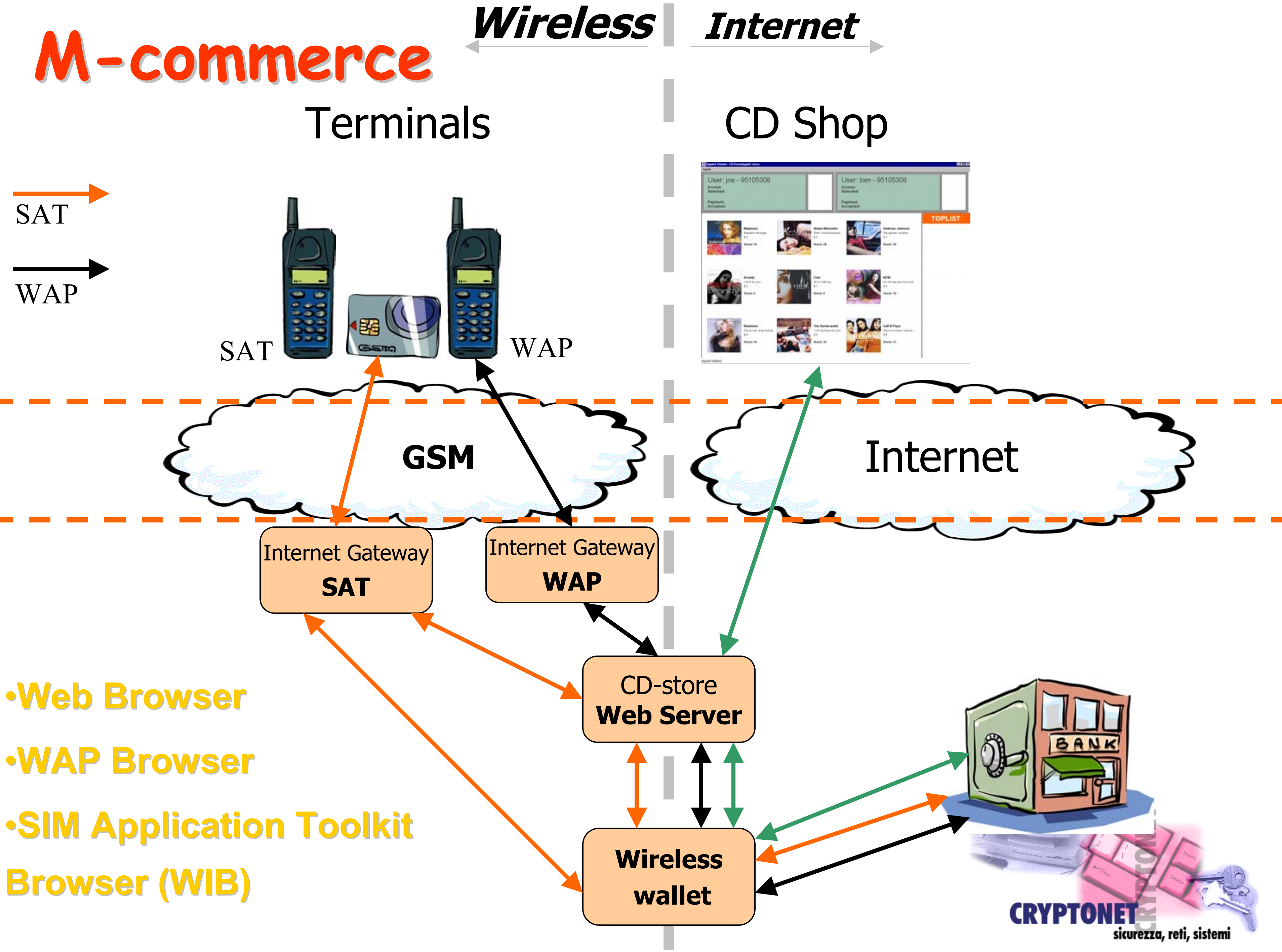
- WAP-mobile are not widespread today
- Phone manufacturers go on selling non-WAP-mobile (less expensive and not perceived add-value)
- Many users do not use WAP features (or unable to)
- No “pure WAP solution” available for client authentication and signing transactions (only with WAP 1.2)
- No push of a signing request to the users mobile phone

Deficiencies of WAP (2)

- We have to use **GSM** (with WAP, if there's)
- ALL mobile phones uses GSM
- We can use **Short Message Services (SMS)**
  - for every operations
  - or just for operations that WAP does not implemented yet
- SMS are more user-friendly than WAP browsers
- Hence, hybrid solution between SMS e WAP

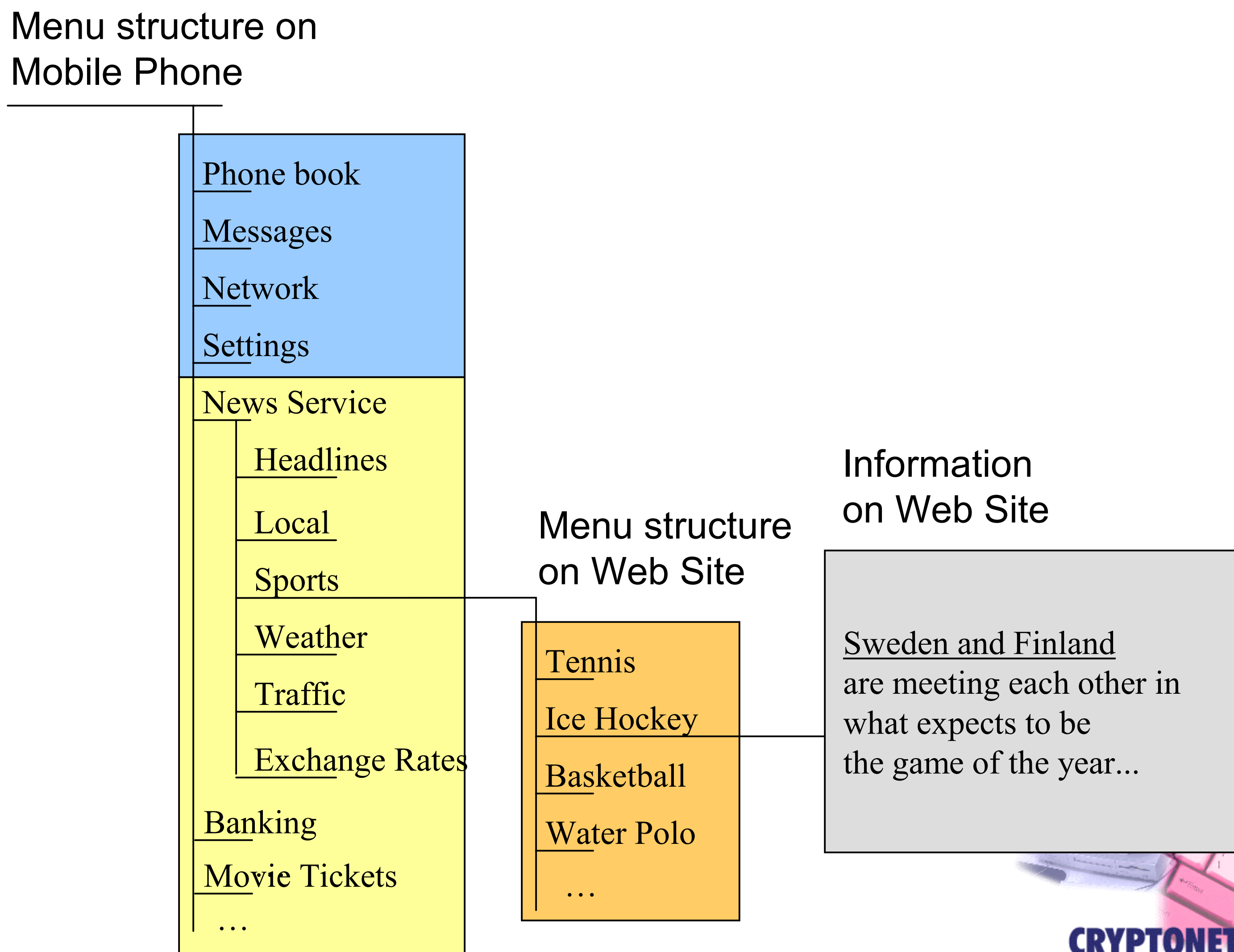
SmartTrust™

M-commerce

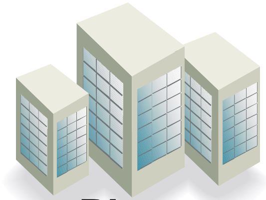
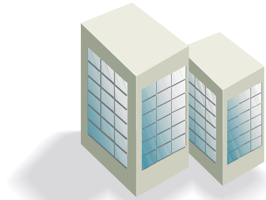
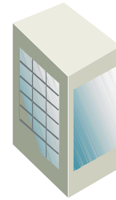
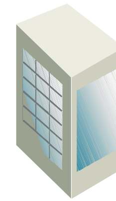


- Web Browser
- WAP Browser
- SIM Application Toolkit Browser (WIB)

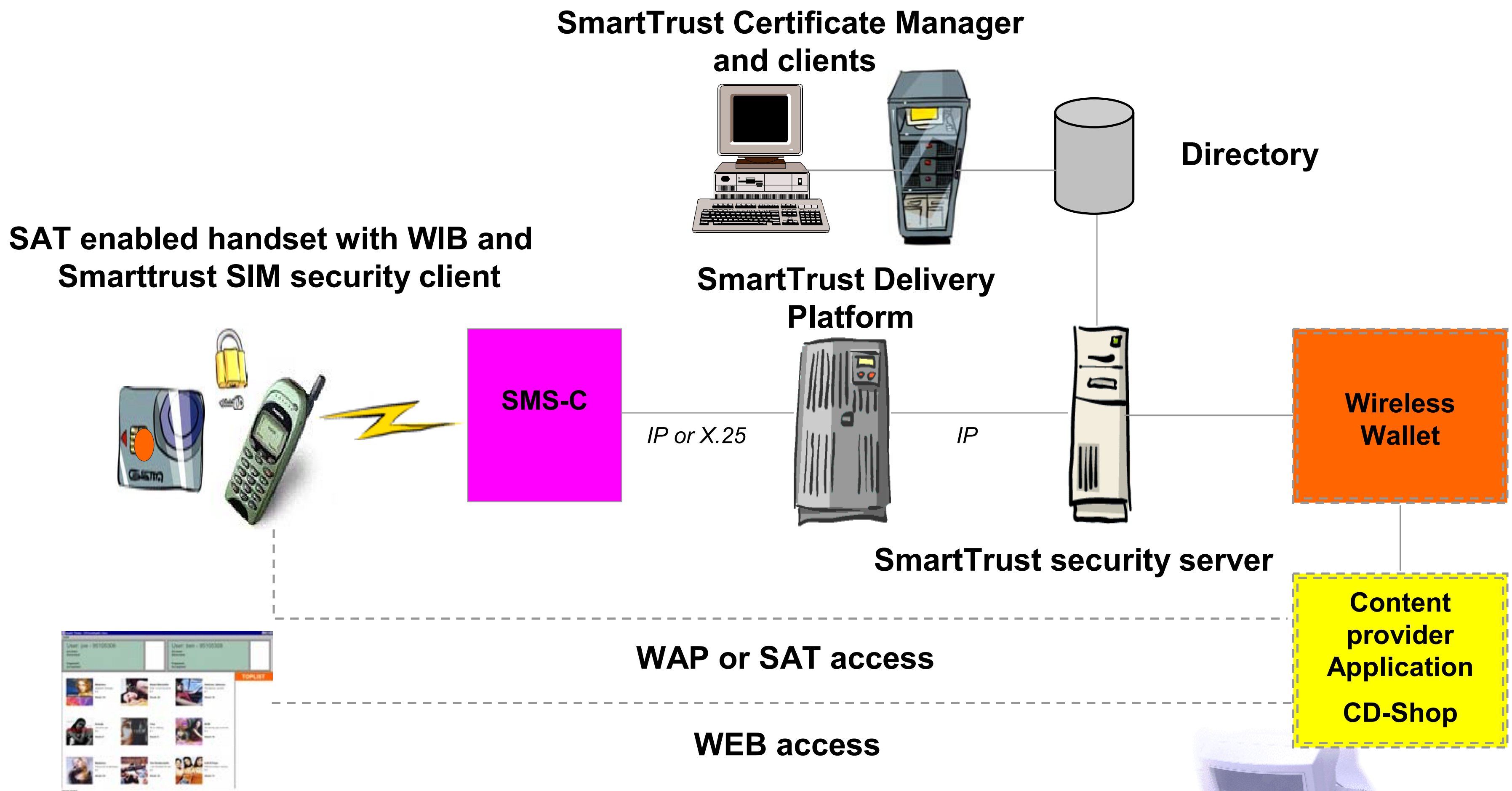
Browsing services located on SIM and/or web-wap site



Key (& Certificate) Insertion Points

 Phone Manufacturer	 Card Manufacturer	 Mobile Operator	 Service Provider	 End user
CA root key and/or certificate may be placed in firmware mask from an image file provided by Certificate Authority	CA root key and/or certificate may be placed on SIM from an image file provided by Certificate Authority End User Encryption key-pair and digital signature key-pair pre-generated and stored on SIM	End User enrollment at Mobile Operator: End User Encryption Public Key and Verification Public Key sent to Certificate Authority for “binding” to certificates. Returned certificates stored on SIM or on the network.	End User enrollment at Service Provider: End User Encryption Public Key and Verification Public Key sent to Certificate Authority for “binding” to certificates. Returned certificates stored on SIM or on the network.	End User enrollment Over the Air: End User Encryption Public Key and Verification Public Key sent to Certificate Authority for “binding” to certificates. Returned certificates stored on SIM or on the network.

Wireless PKI System

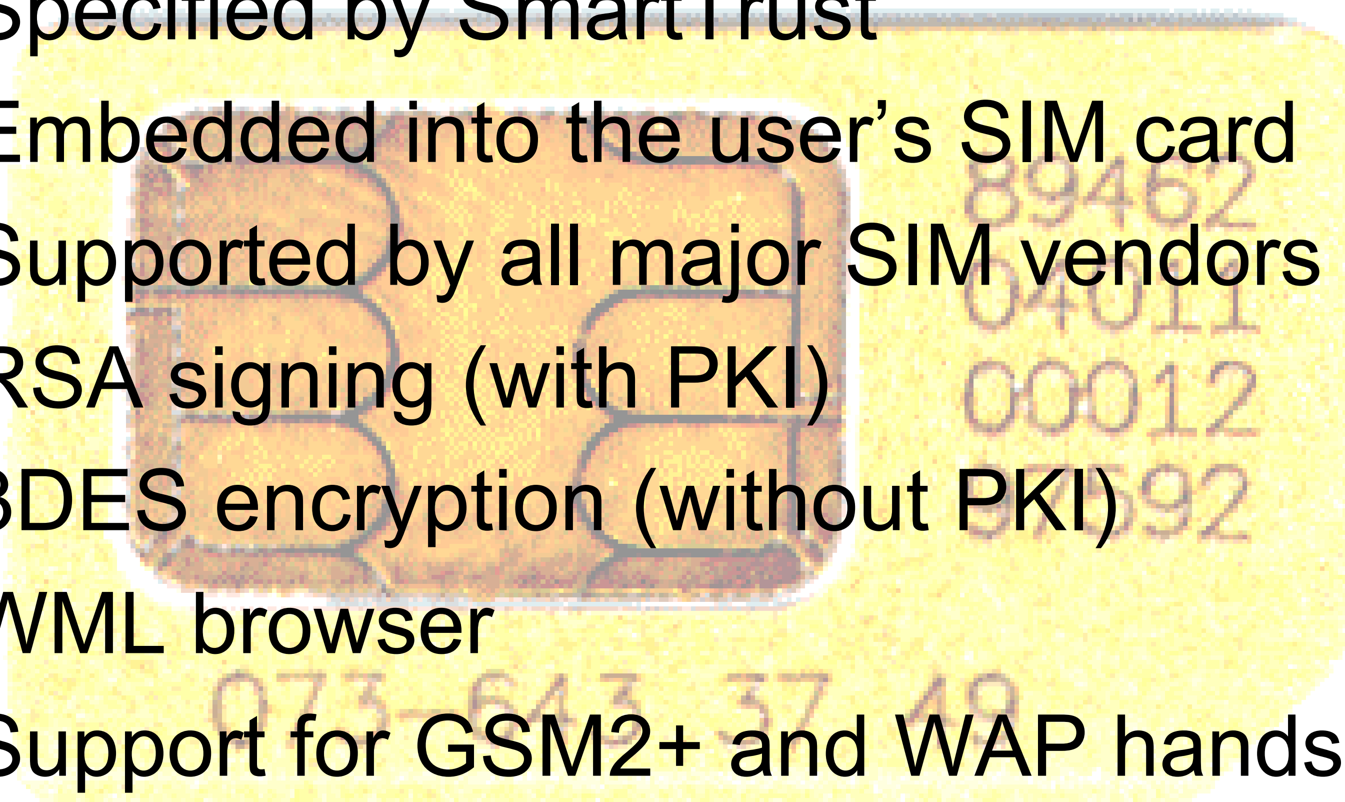


SIM=Subscriber Identity Module

SAT =SIM Application Toolkit

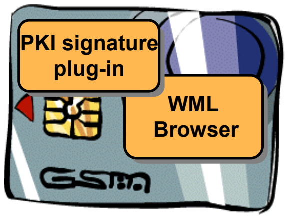
WIB=Wireless Internet Browser

SmartTrust SIM Security Client

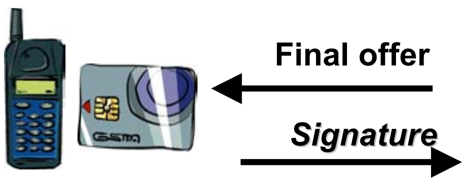


- Specified by SmartTrust
- Embedded into the user's SIM card
- Supported by all major SIM vendors
- RSA signing (with PKI)
- 3DES encryption (without PKI)
- WML browser
- Support for GSM2+ and WAP handsets

The PKI signing procedure



Purpose:
True non-repudiation



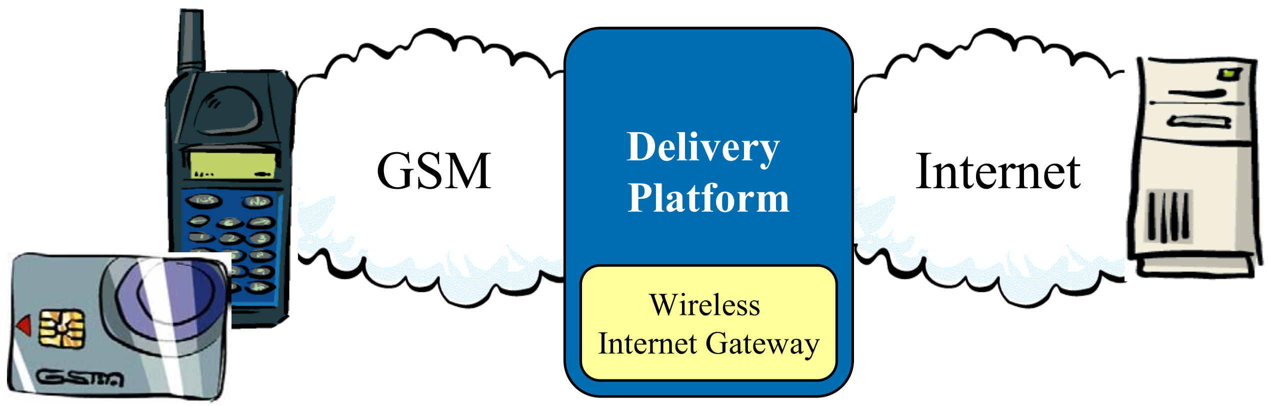
Confirmation of order

- **User receives message**
- **The PKI signature plug-in:**
  - **displays message (final offer)**
  - **requests and verifies user pin-code**
  - **performs hash on message**
  - **runs RSA on the hash → *signature***

...all in one operation by plug-in

- Signature is verified by Operator or Merchant

SmartTrust Delivery Platform



3DES Encryption/Decryption

RSA Signature

End-to end security

3DES Encryption/Decryption

SignatureVerification

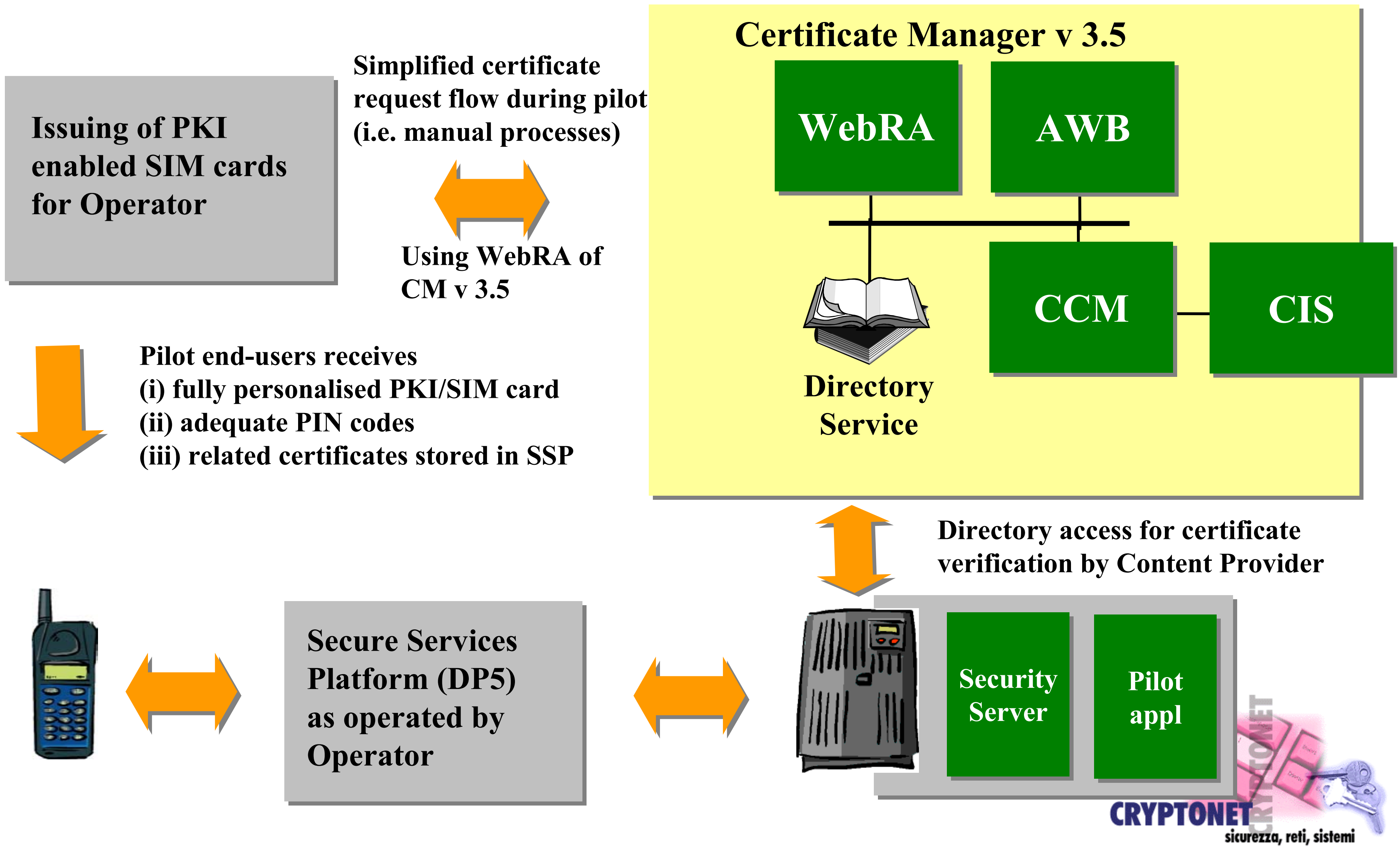
Wireless Internet Browser GSM 03.48

GSM 03.48 / WTLS

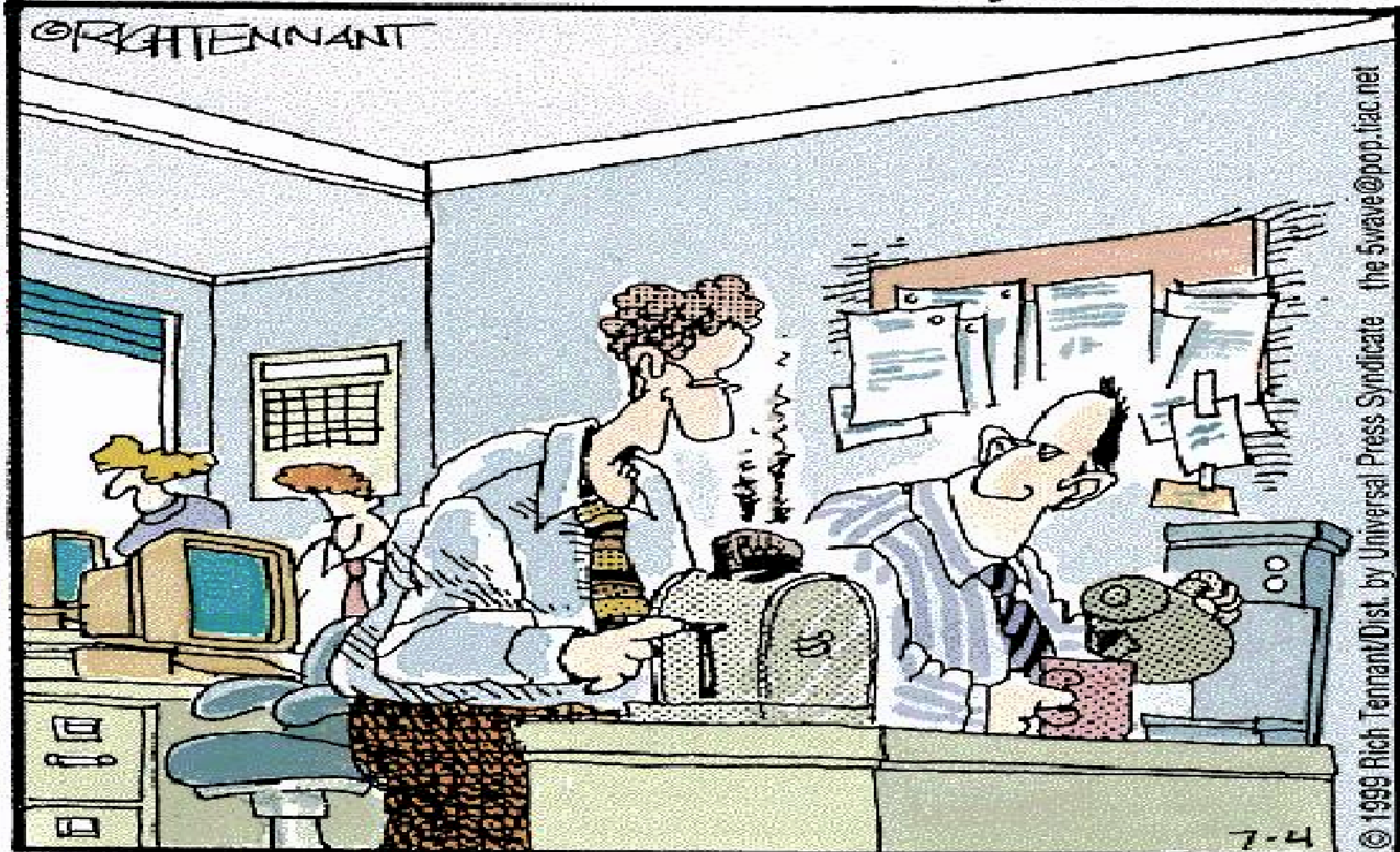
SSL

SSL Server
CRL & CTL access

Overview of Wireless PKI pilot: CA details



The 5th Wave By Rich Tennant



"I don't know how it happened, but there's an applet in the toaster and some guy in Norway keeps burning my toast."

Question Time

mirko.tedaldi@cryptonet.it

CRYPTONET
sicurezza, reti, sistemi

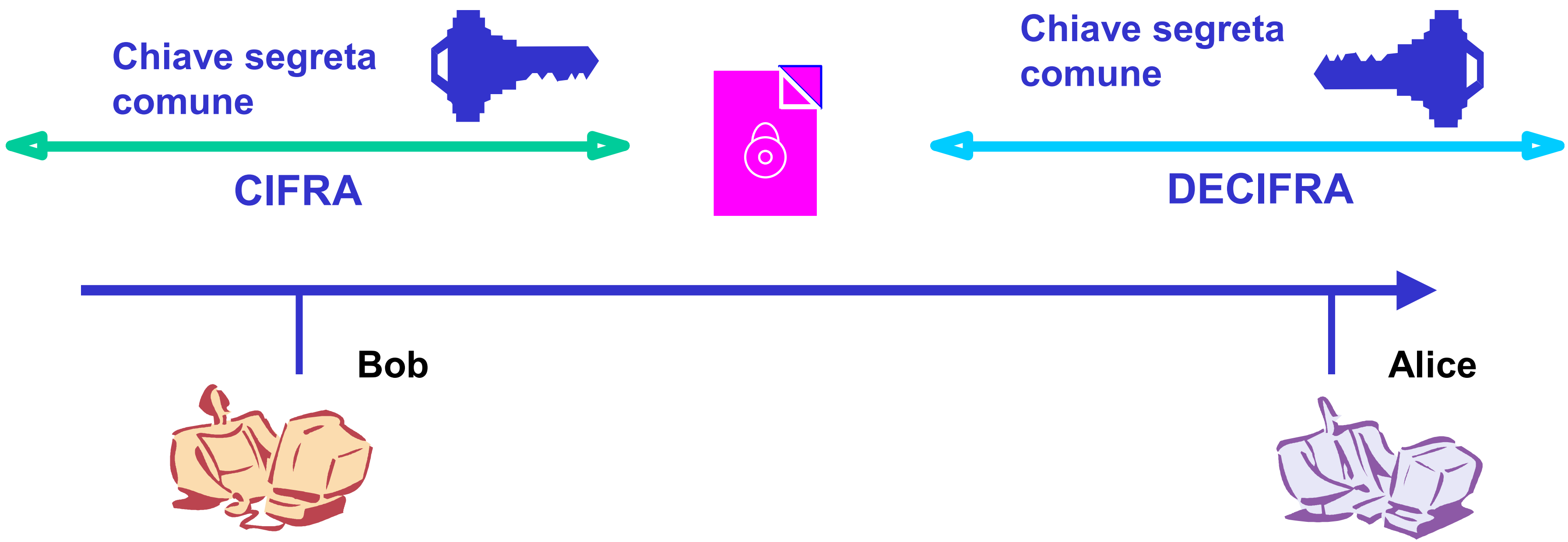
Altro materiale

I due tipi di algoritmi crittografici

- **Crittografia simmetrica (o a chiave segreta)**: utilizza **una sola chiave** crittografica che deve essere posseduta sia dal mittente sia dal destinatario del messaggio

- **Crittografia asimmetrica (o a chiave pubblica):** utilizza **una coppia di chiavi** (una pubblica e l'altra privata) possedute entrambi da un unico proprietario

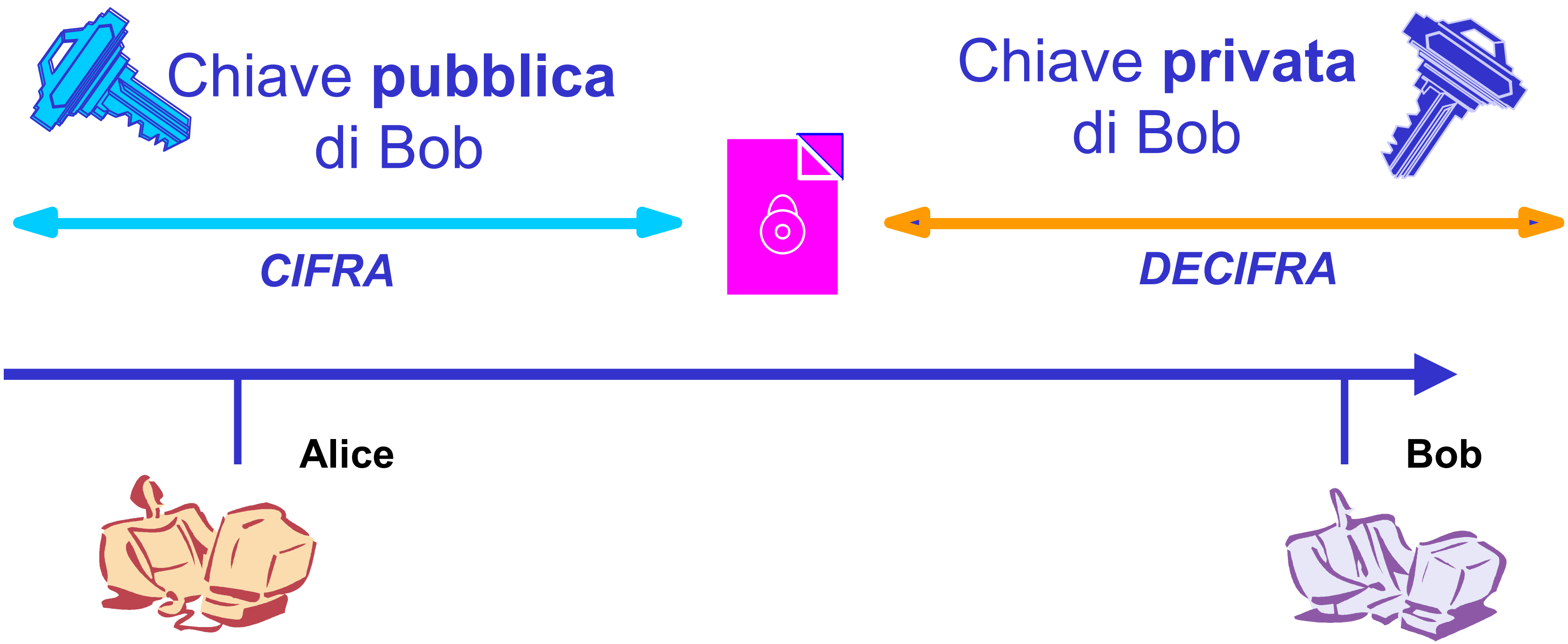
La Crittografia Simmetrica



Bob e Alice condividono una chiave segreta comune

La Crittografia Asimmetrica

CONFIDENZIALITÀ

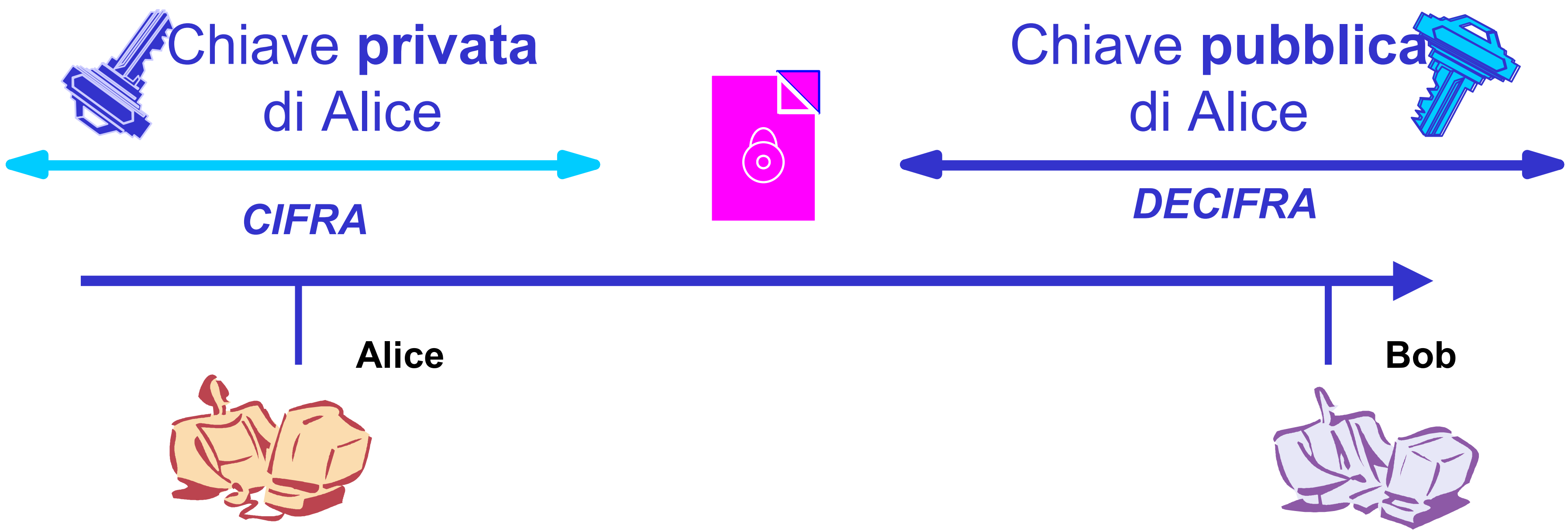


Solo Bob può decifrare il documento, perché solo lui possiede la chiave privata

CRYPTONET
sicurezza, reti, sistemi

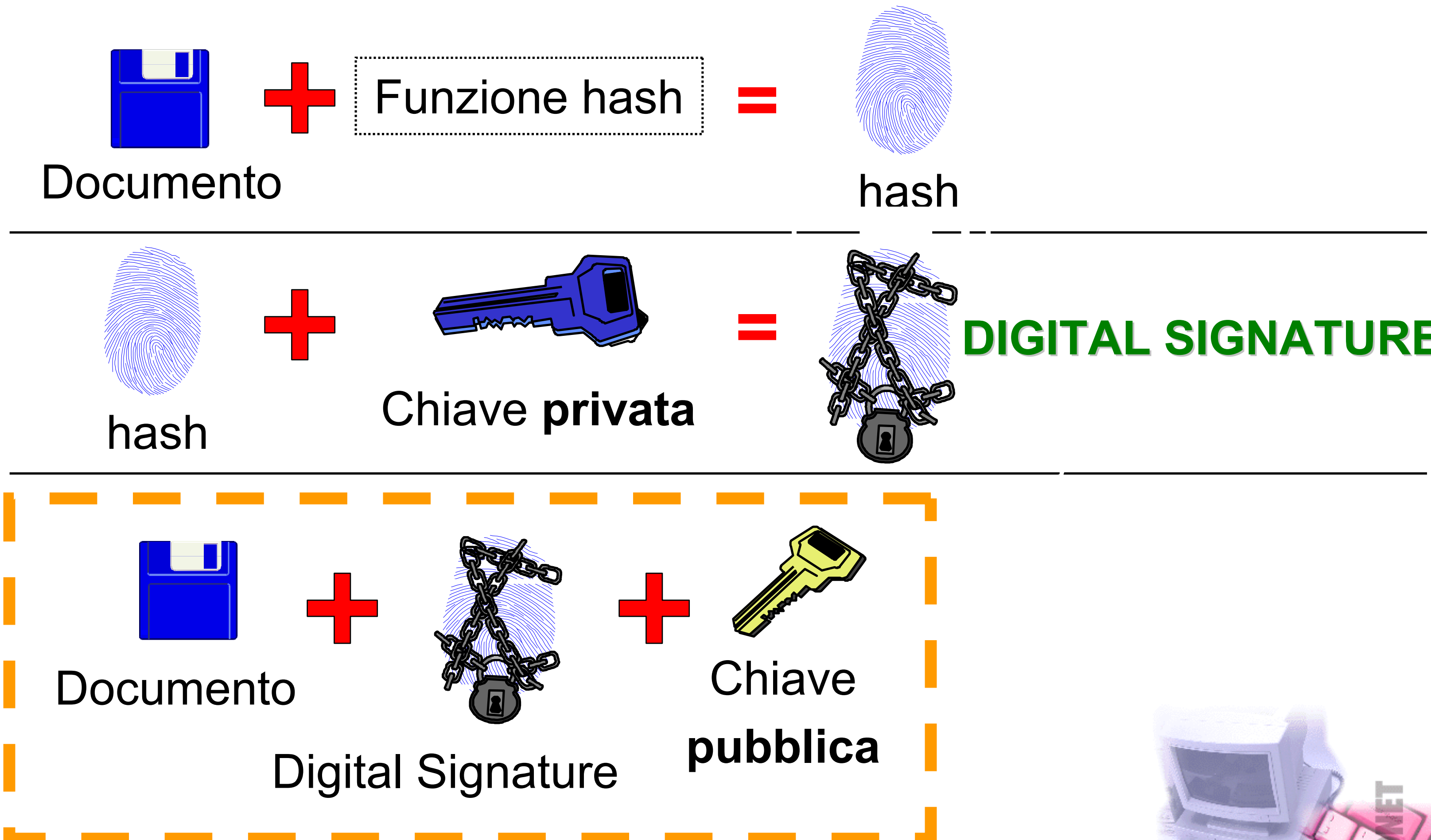
La Crittografia Asimmetrica

AUTENTICAZIONE



Bob è sicuro che il messaggio è stato cifrato da Alice perché solo lei possiede la sua chiave privata

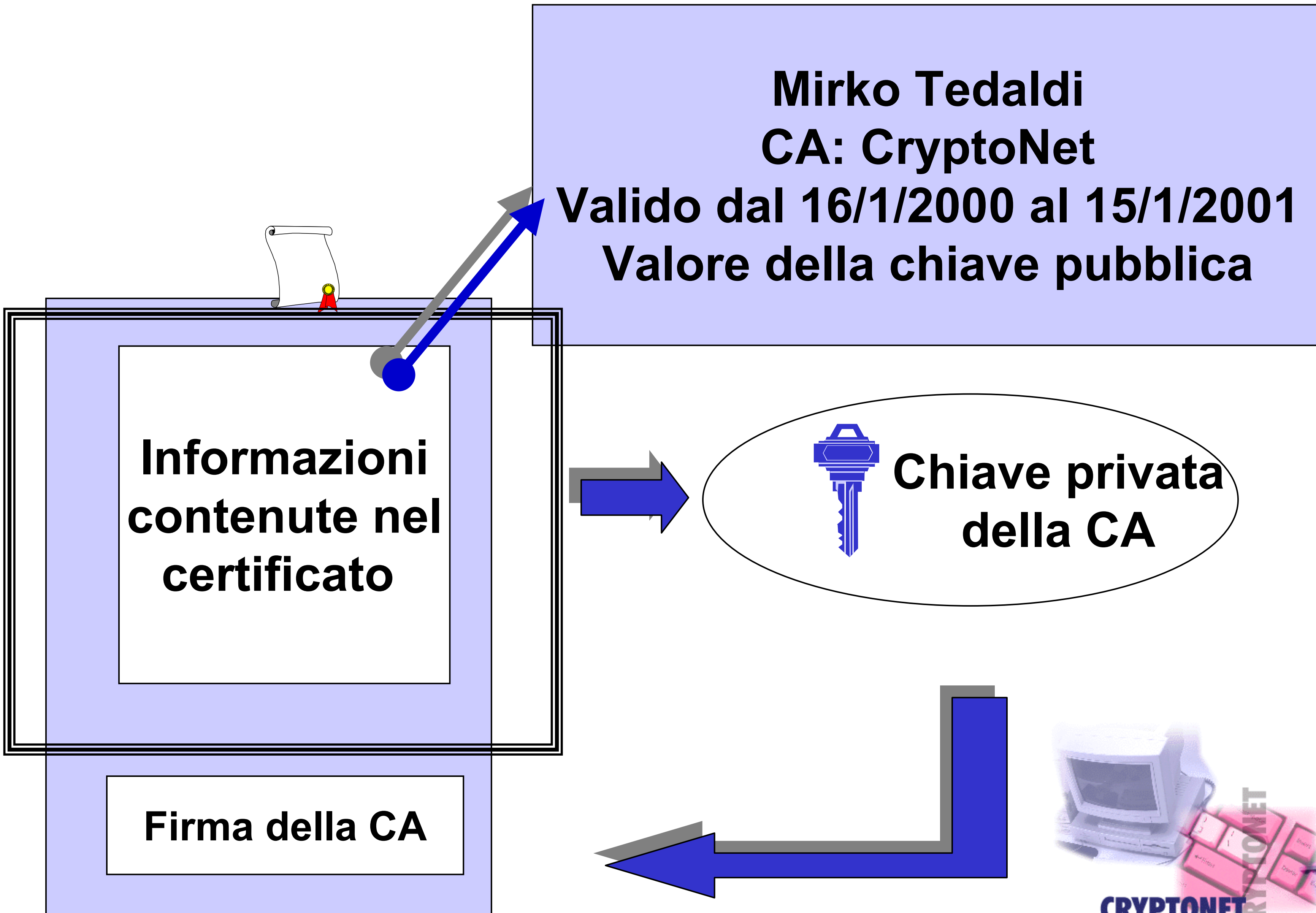
Creazione della Firma Digitale



CRYPTONET
sicurezza, reti, sistemi

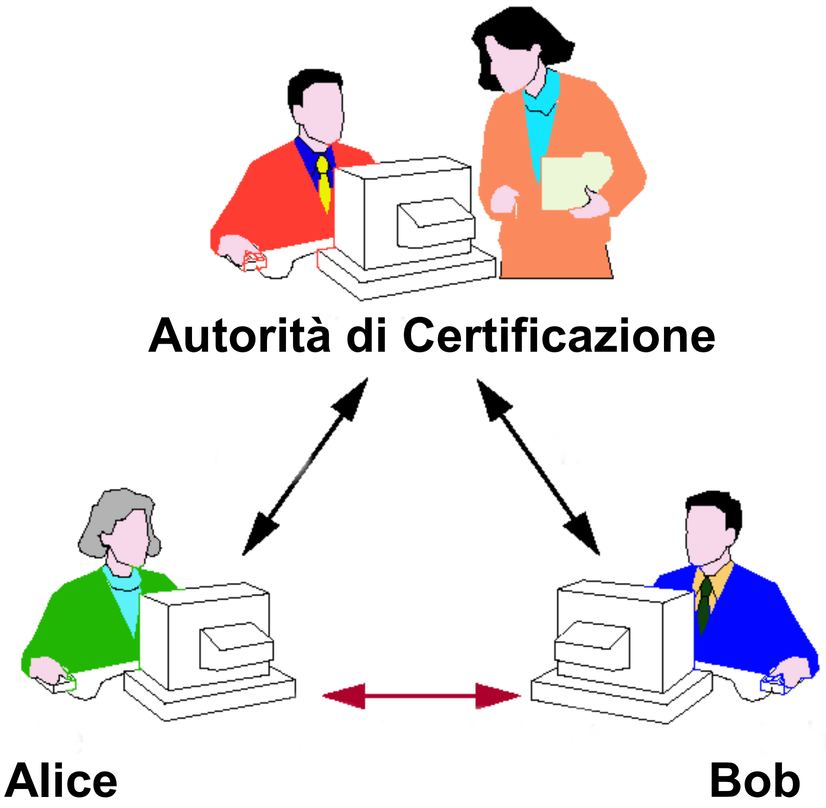
Verifica della Firma Digitale

I Certificati Elettronici

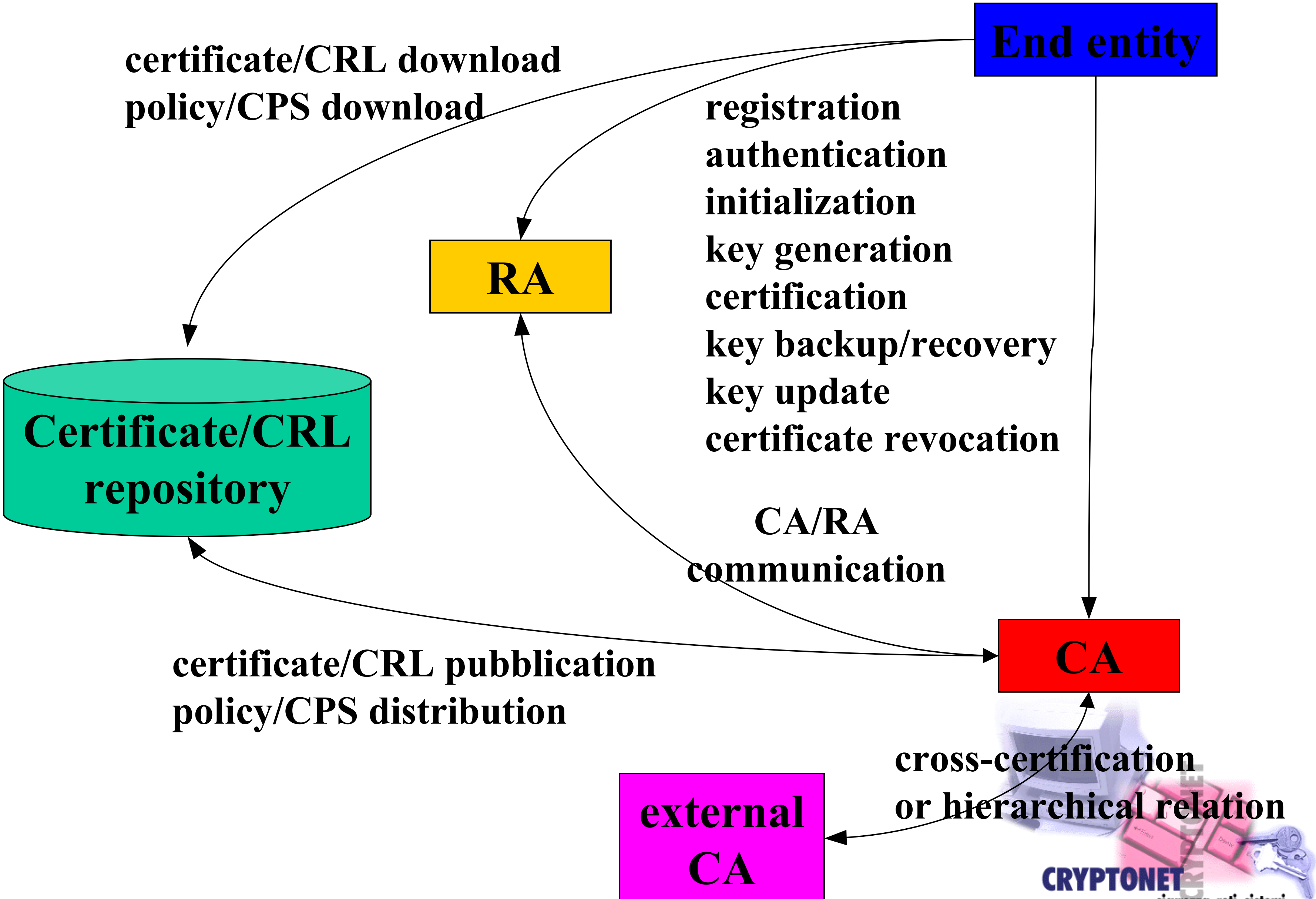


Third-Party Trust

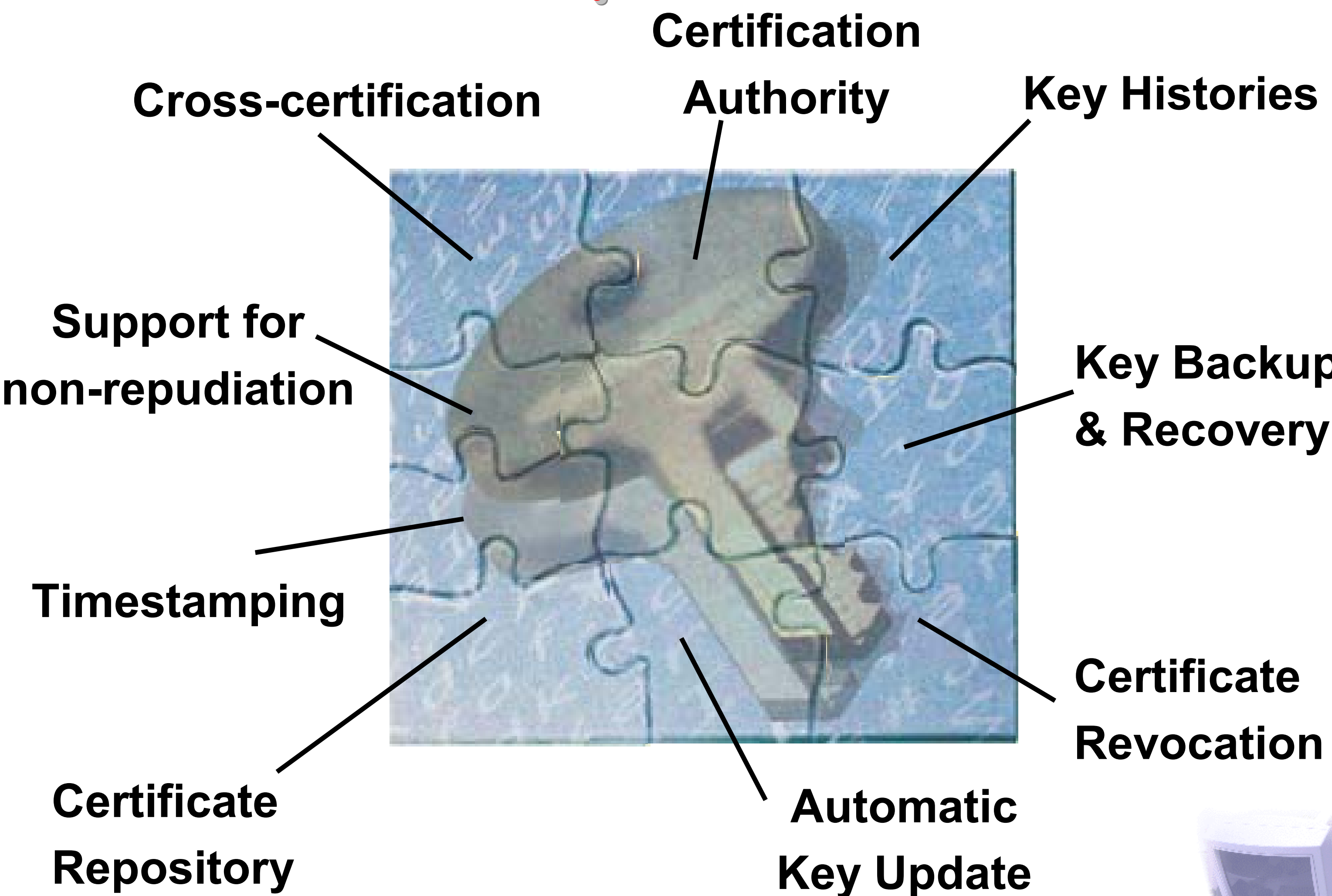
Garantisce la **corrispondenza tra chiave pubblica e soggetto** attraverso i **certificati digitali**



Public Key Infrastructure



Requirements

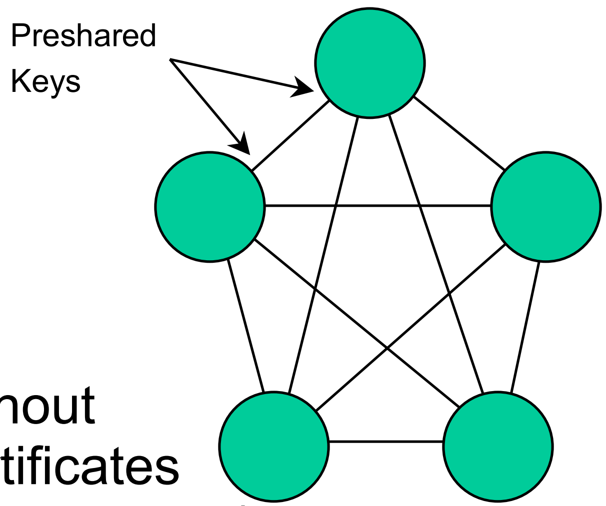


Why is PKI important to VPN?

- It is relatively easy to build a secure pipe or tunnel between two nodes or users on a **public network**
- Unless you know exactly who is at both ends of the pipe it has little value (**initial authentication** is fundamental)
- **Digital certificates** provide a means to strongly authenticate users and devices in a VPN tunnel
- A **managed PKI** provides a scalable platform upon which to build large, secure, and trusted VPN's.

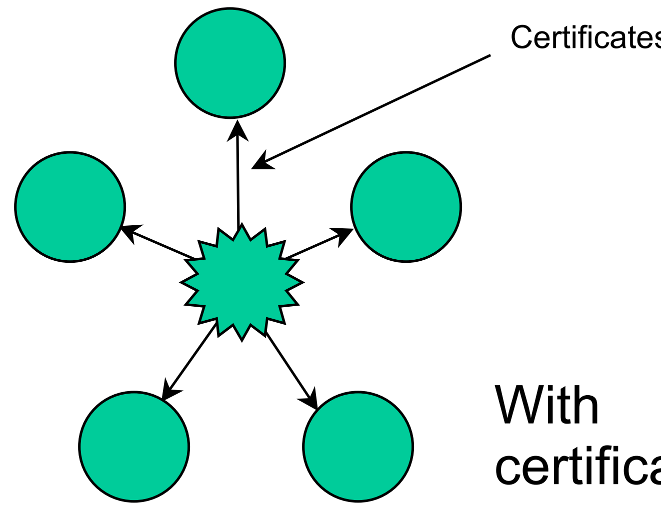
Scalability

- VPNs do not scale without using public-key certificates



Without Certificates *(fully-meshed)*

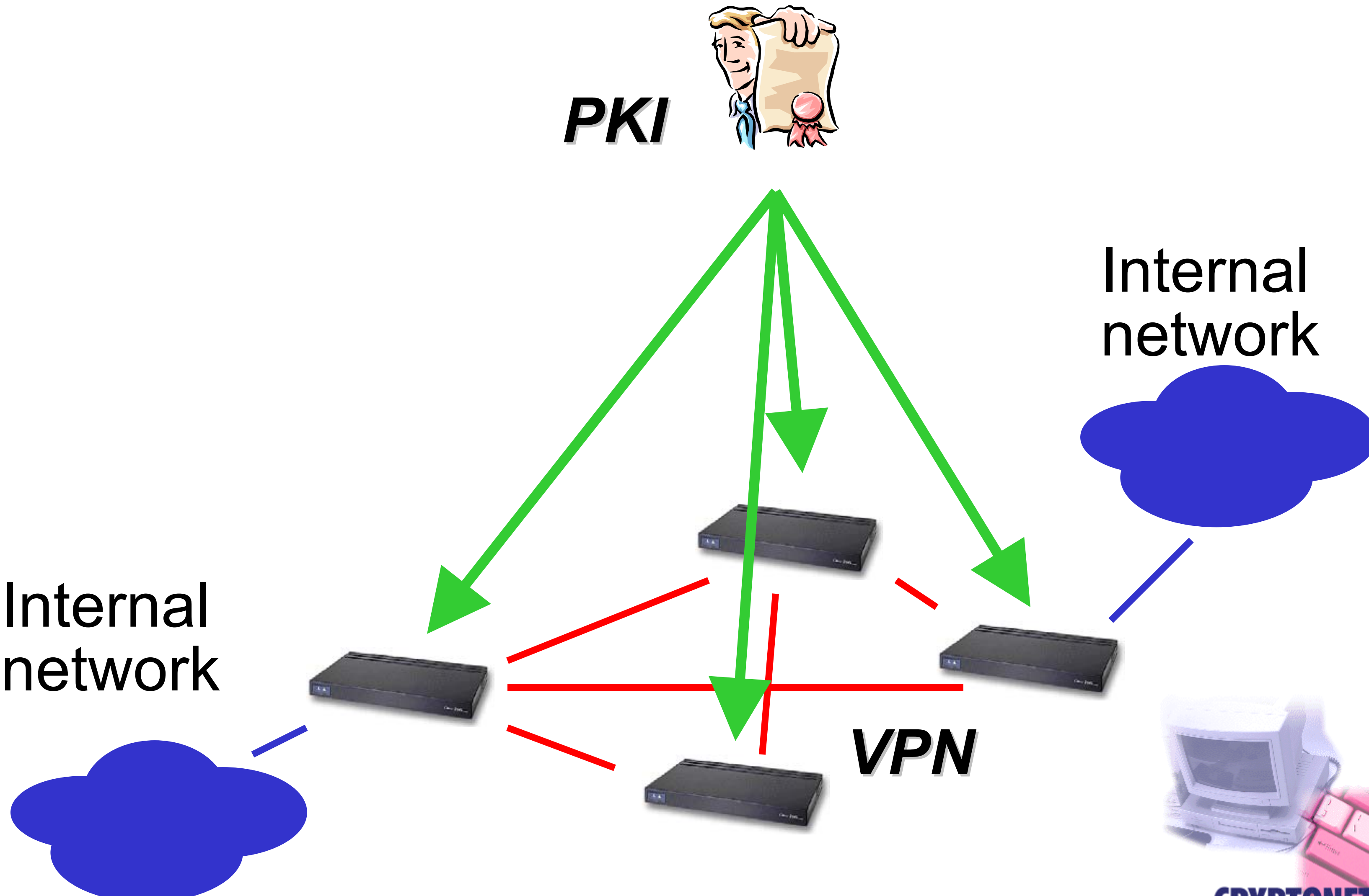
Effort $\propto n^2$



With certificates

Effort $\propto n$

VPN + PKI



CRYPTONET
sicurezza, reti, sistemi