

**Sagem Orga**  
Strong, Global, Innovative.



# SIM card securing Internet based application



**Didier Sérodon**  
Chief Technical Officer

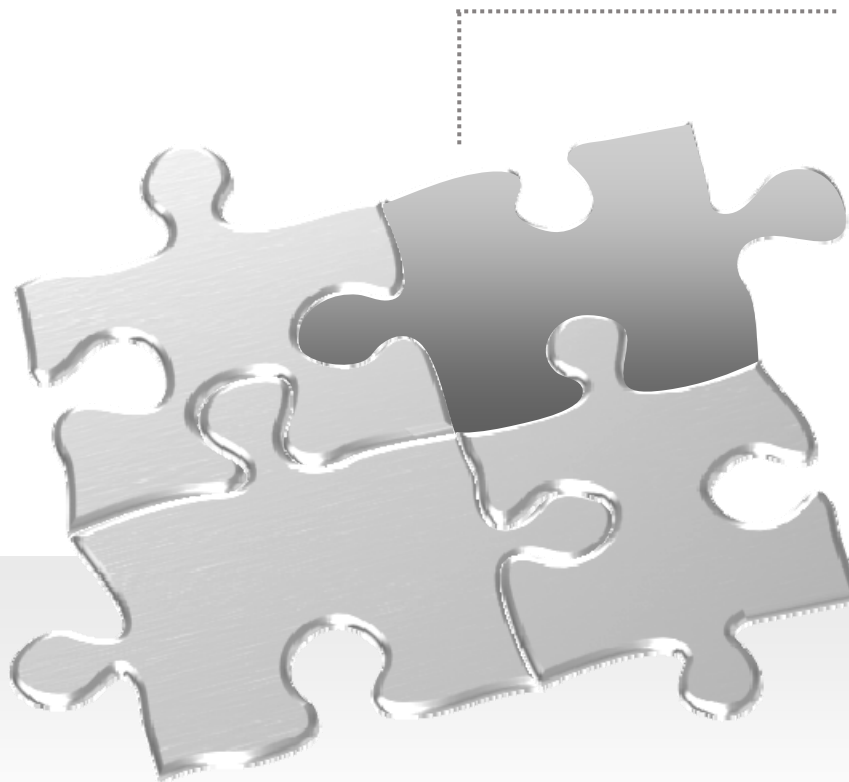
# Internet keeps changing its environment

## Convergence

- Mobile and Fixed Network merger,
- Devices handle multiple technologies (GSM, 3G, Wi-Fi, ...),
- Netbooks,
- Same Services available everywhere (VoIP, Streaming, ...).

## Security in question

- Hacking, phishing, an everyday reality,
- More than 50% of transaction stopped when Credit Card details have to be entered.
- Login / Password ...



## Huge Opportunity

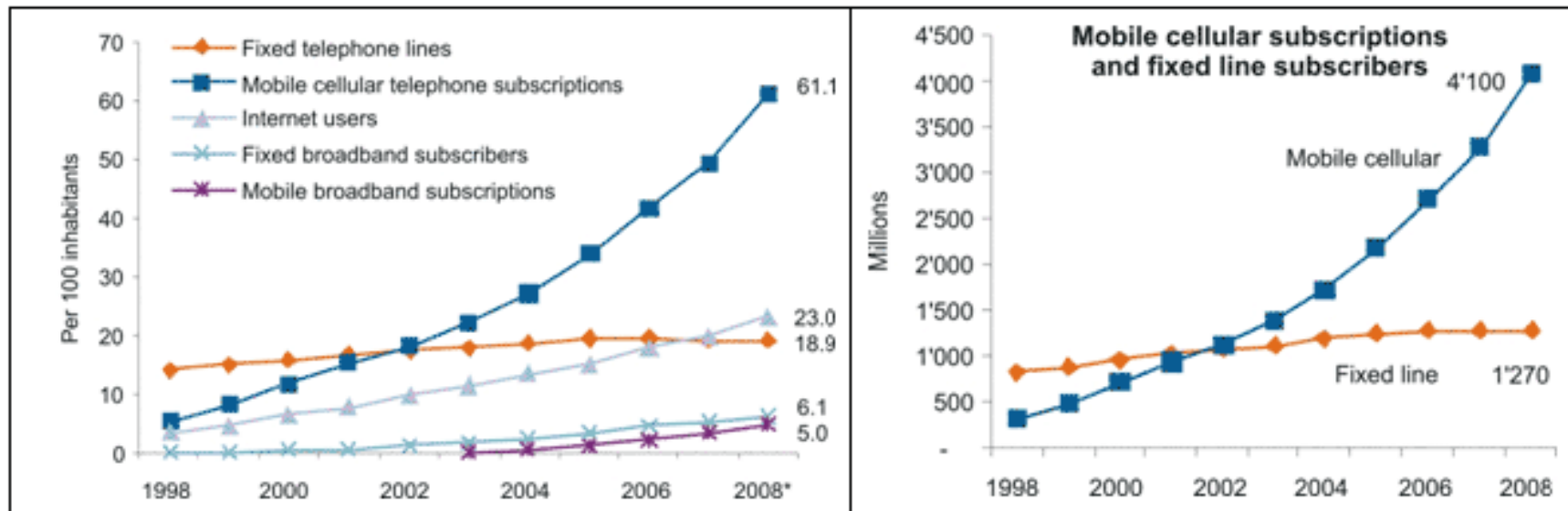
- Forecast for IT security market \$ 12B in 2010,
- Internet is becoming The Channel
- More than 35 000 WEB sites Open ID compatible.

## Smart Card, secure token

- The SIM card for GSM, 3G
- The PayTV conditional access device,
- The Payment Token (EMV, Paypass, ...),
- Corporate Badge, Access.

# Mobile is winning the battle

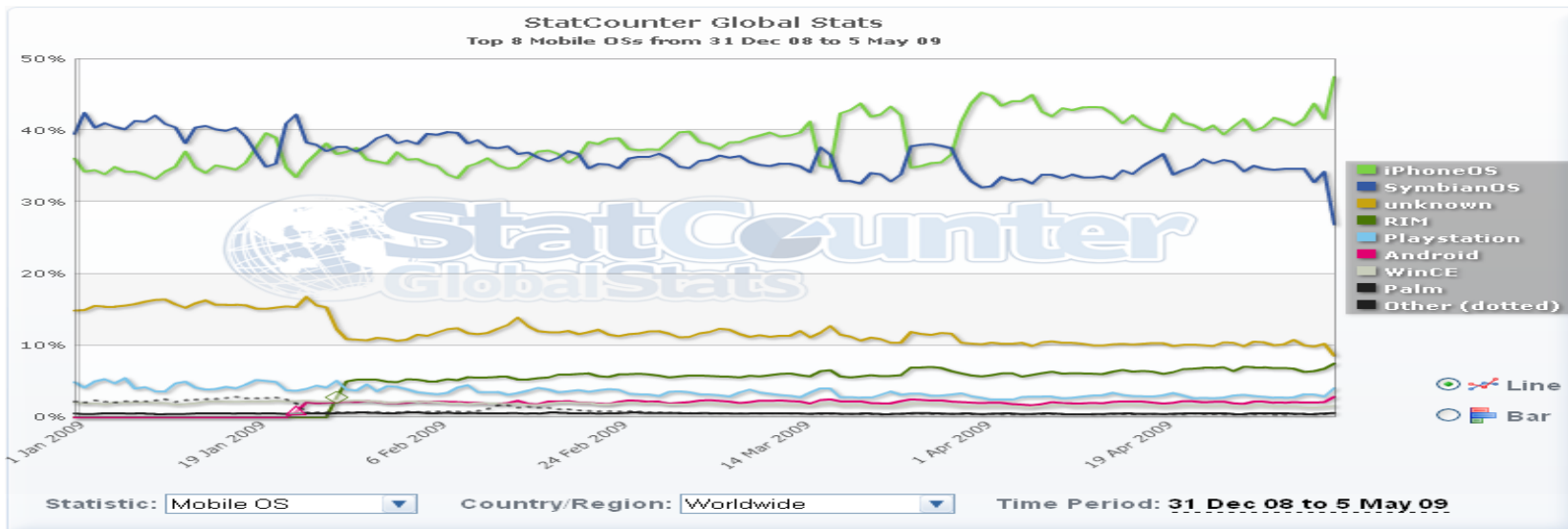
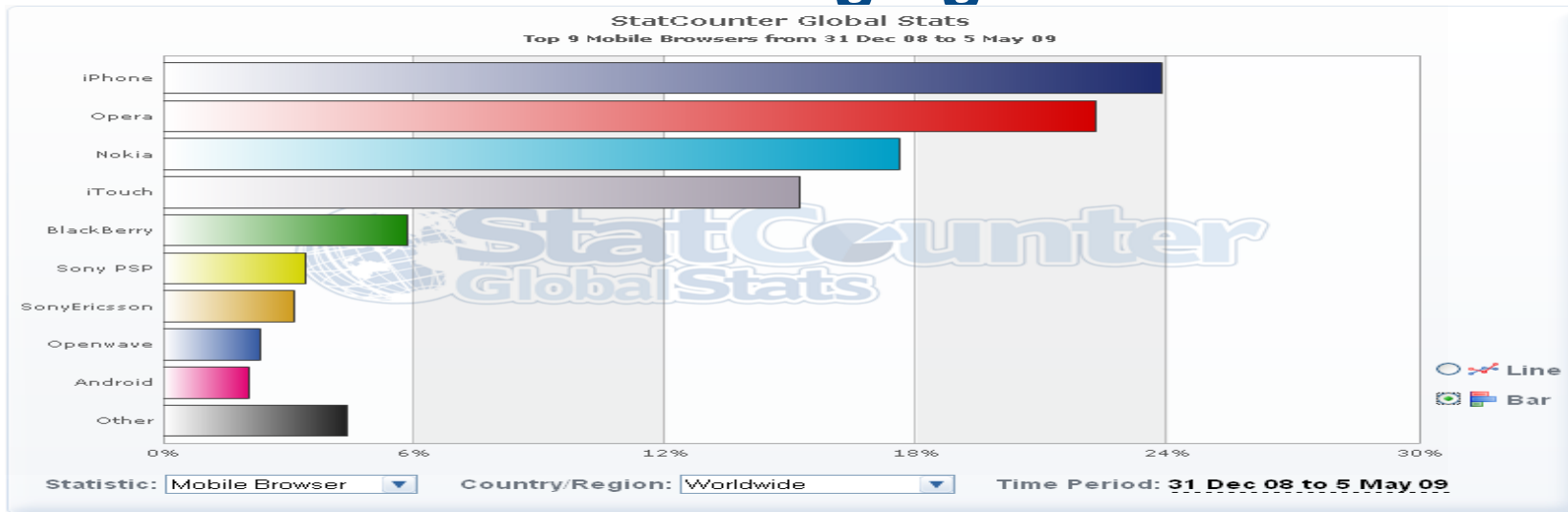
## Global ICT Developments



Note: \* Estimates.

Source: ITU World Telecommunication/ICT Indicators database.

# Mobile Internet is changing



# Why do we need Secure Internet?

## E-Commerce

- E-payment
- E-Banking



## E-Gaming

- Poker
- Gambling games



## Single Sign On

- MNO WEB portal
- Bank internet site
- Any OpenID internet site



## Corporate services

- Intranet
- E-mail
- Corporate phonebook



# ■ ■ ■ ■ TLS Tandem: the easy way to secure Internet

## Postulates

- ▶ Make the SIM card a secure token for the WEB
- ▶ Single Sign On solution re-enforced by the mean of a SIM card
- ▶ Compatible with standards and usual WEB technical environment (Open ID and HTTPS)
- ▶ A solution to make the MNO a key player for the security of WEB services

## Partner

- ▶ Ethertrust market software for smart cards and design innovative solutions that strengthen the security of WEB applications while dramatically simplifying their use.



# USB Companion, a device for convergence



# How would it work?

Insert SIM in  
USB dongle

Plug the dongle  
to laptop

Connect to  
internet.

1- Automatic authentication

2- Secure connection set up

3- Get access to WEB services

4- Use services

TLS Tandem javacard  
applet

Memory for Internet  
Everywhere software

TLS Tandem Proxy

Java OS

USB dongle with SIM card  
reader (PCSC) and HSDPA  
modem

Windows / Mac / Linux OS



# Role of the SIM in our solution

1

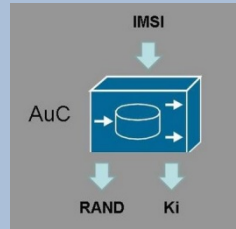
Store certificates



- At registration step the SIM applet will receive and store the WEB service certificate

2

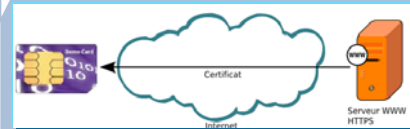
Authentication



- Exchange user credential With security provider to Operate the mutual authentication

3

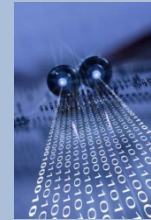
Set up secure session



- An HTTPS or SSL session Is set up by the SIM card

4

Transfer session keys



- The session key and encryption keys are Transmitted to proxy

5

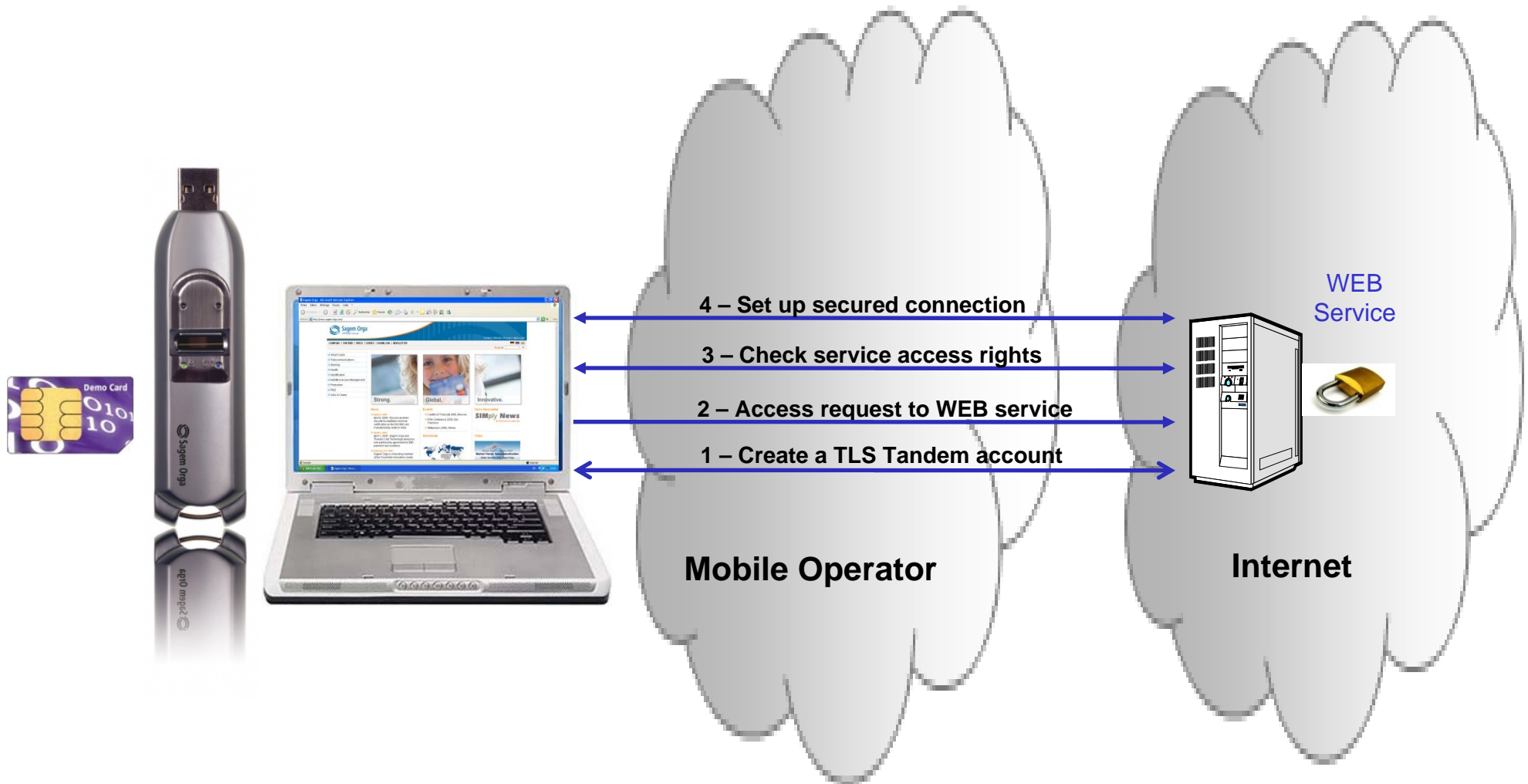
Service



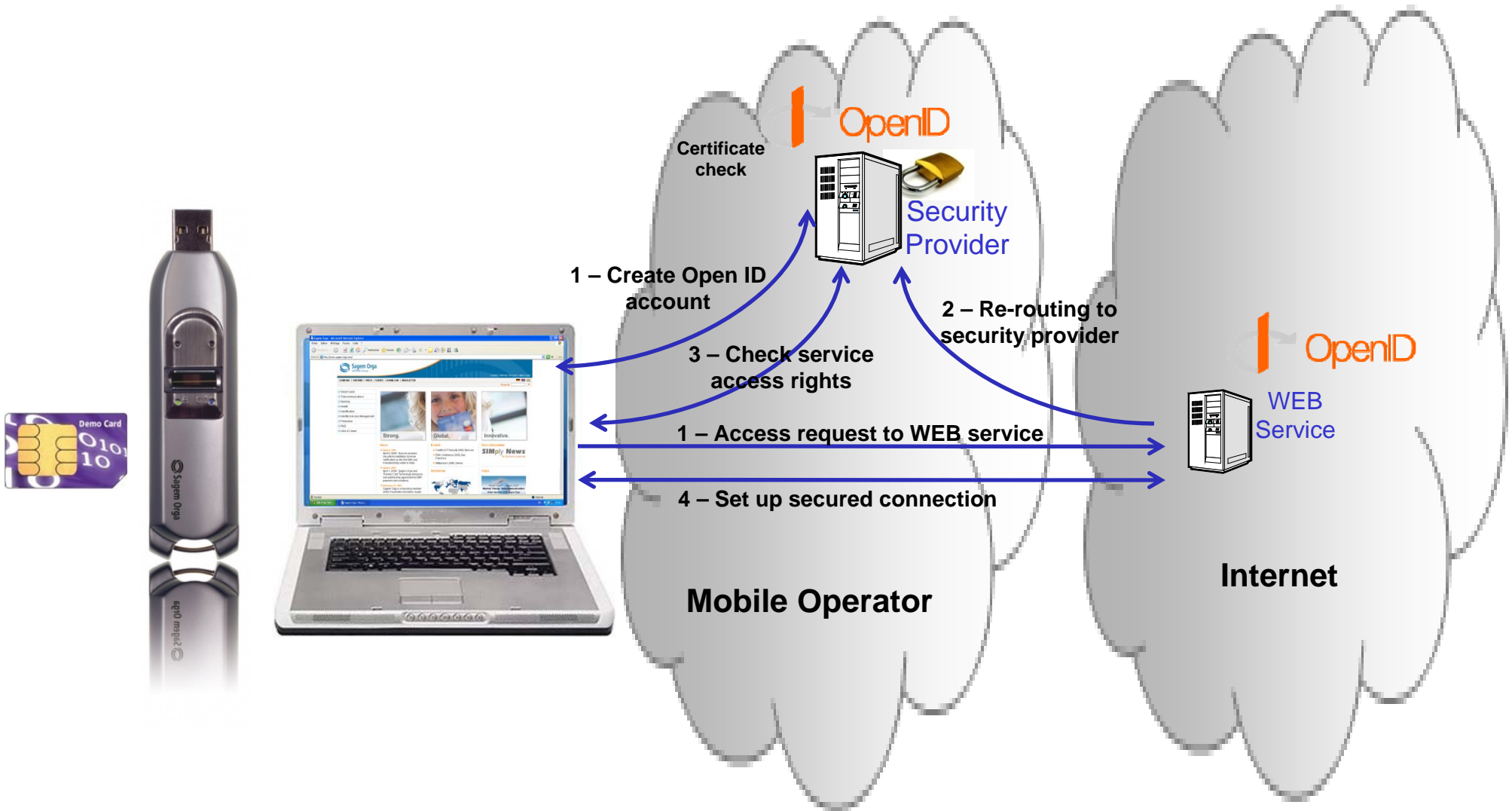
- The SIM contains a payment application used for the e-transaction

Optionally

# ■ ■ ■ ■ Solution architecture: case 1, TLS Tandem



# Solution architecture: case 2, Open ID



# User experience



Secure SSL session



Sagem Orga – CTST – New Orleans, May 2009

# Business model

**1**

Connect token and log to my MNO porta



**2**

Access to a partner web store

**4**

Cash back

**3**

« One click » payment



# Benefits

## The end user

- ▶ Simplify and protect its life on Internet
- ▶ No more need for login & password, a device and the PIN
- ▶ Phishing killer solution

## The MNO

- ▶ Become an Internet security provider – Open ID provider
- ▶ Secure usage of its WEB services
- ▶ Trace usage of WEB services for better billing
- ▶ Increase usage of WEB services

## Technical

- ▶ A unique and secure place to deploy the solution to ensure more security: every single byte flowing out of the SIM card is encrypted
- ▶ Spyware are blind, the computer is just a « plug » Authentication & Encryption algorithms are entirely computed in the SIM Card
- ▶ Compatible with existing infrastructure and standards

# Conclusion

- ▶ **The TLS SIM card, the convergence solution for WEB services**
  - ▶ a secure token to provide more security to WEB services,
  - ▶ Portable, and easy to use,
  - ▶ Standards fully defined and already implemented (EAP-TLS)
  - ▶ Unique solution for Fixed + Mobile browsing
  - ▶ Opened to Security and Value Adding Applications
    - ▶ Payment
    - ▶ SSO
    - ▶ Loyalty
    - ▶ ...

**Sagem Orga**  
Strong, Global, Innovative.

