NUOVE **TECNOLOGIE**,
risorsa per la **comunità ecclesiale**

Montesilvano 25-27 gennaio 2005

Sicurezza informatica

A cura di Roberto Pompei, SICEI
Incaricato dei progetti software, del sistema di rete e della sicurezza dati

pompei@chiesacattolica.it

Cosa si rischia

- **Blocco dei sistemi** dovuti a:
  - Virus informatici
  - Rallentamenti/intasamenti delle connessioni
  - Spamming
- **Furto di identità digitali e password** e utilizzo non autorizzato delle stesse
- **Furto di informazioni riservate o “sensibili”** come codici bancari e archivi di dati personali
- **Perdita di dati** dovuta a errori o eventi accidentali

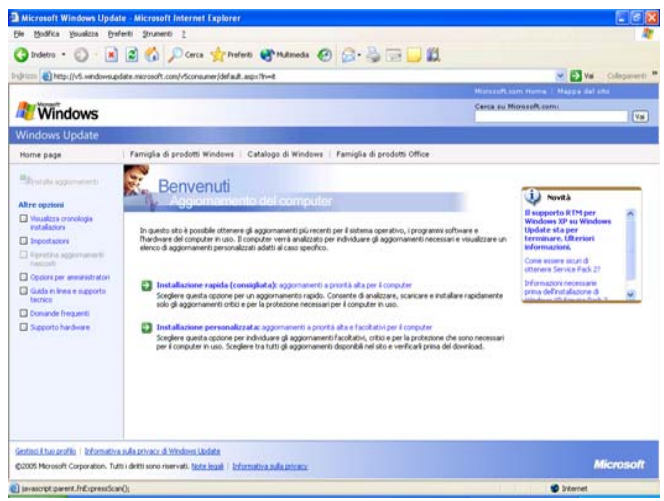
Rimedi e contromisure

- Individuare ed applicare tutta una serie di strumenti (hardware e software) che :
  - riducano quanto più possibile il rischio di manomissione dei propri sistemi e di utilizzo indebito di informazioni.
  - diano sufficienti garanzie sul recupero dei propri dati in caso di perdita (accidentale o meno).

dieci consigli per un sistema sicuro

1. **Sicurezza fisica:**
   - Il luogo dove si trovano le apparecchiature (con particolare attenzione a quelle che contengono i dati) deve essere convenientemente protetto.

2. **Sicurezza software del S.O.:**
   - aggiornamento costante del sistema operativo utilizzato (es. Windows Update)



dieci consigli per un sistema sicuro

3. **Adozione / aggiornamento di software di protezione da attacchi “interni”:**
   - antivirus
   - antidialer
   - antispyware

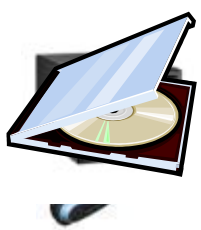
4. **Adozione / aggiornamento di software di protezione da attacchi “esterni”:**
   - firewall

dieci consigli per un sistema sicuro

5. Copie di backup delle proprie informazioni:

- Utilizzo di software integrato nel S.O. (es. Backup di Windows 

) o di prodotti a sè
- Supporti di memorizzazione:
  - ***Floppy*** (in via di “estinzione”)
  - ***Chiavi USB:*** sostituiscono i floppy ma NON garantiscono un’alta affidabilità
  - ***CD/DVD:*** per copie di dimensioni ridotte e per salvataggi non frequenti (settimanali/mensili)
  - ***Nastri:*** per uso aziendale dove va archiviata una consistente quantità di dati o dove il backup è frequente (giornaliero)



dieci consigli per un sistema sicuro

6. Meccanismi di protezione per l'accesso

- ***al PC:*** password del BIOS

- ***alla rete LAN:*** password, token o, in generale, sistemi di autenticazione biometrica

- ***ai dati:*** password o token + crittografia

dieci consigli per un sistema sicuro

7. **Internet (e connessioni remote in genere):**
   - verifica preventiva dei siti visitati
   - utilizzo del firewall
   - NO ai “click selvaggi” soprattutto su finestre di pop-up non richieste
   - Particolare attenzione alla comunicazione di propri dati personali o di dati bancari
   - dare maggiore fiducia ai siti “sicuri” (https://) es. ***intranet.chiesacattolica.it***)
8. **Posta elettronica:**
   - Attenzione alle mail provenienti da mittenti sconosciuti e soprattutto a quelle con allegati NON richiesti
   - Utilizzare prodotti antispamming (o appoggiarsi a server di posta elettronica che gestiscano l’antispamming)

dieci consigli per un sistema sicuro

9. **Tenersi aggiornati:**
   - Utilizzo di tech-net/forum (es. security bullettin di Microsoft)

10. **Formazione del personale**
    - corsi interni per l'utilizzo degli strumenti
    - educazione alla sicurezza

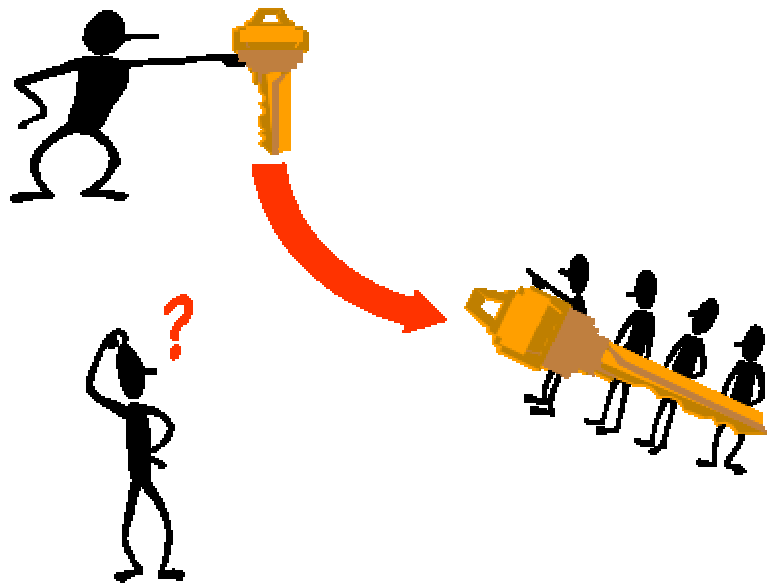
NUOVE **TECNOLOGIE**, **risorsa** per la **comunità ecclesiale**

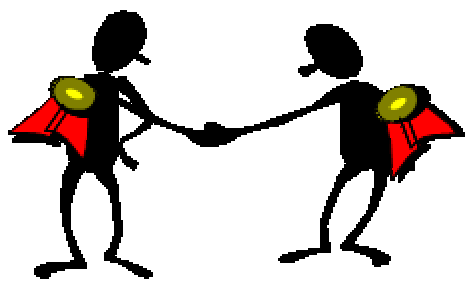
Montesilvano 25-27 gennaio 2005

Smart Card e Firma Digitale

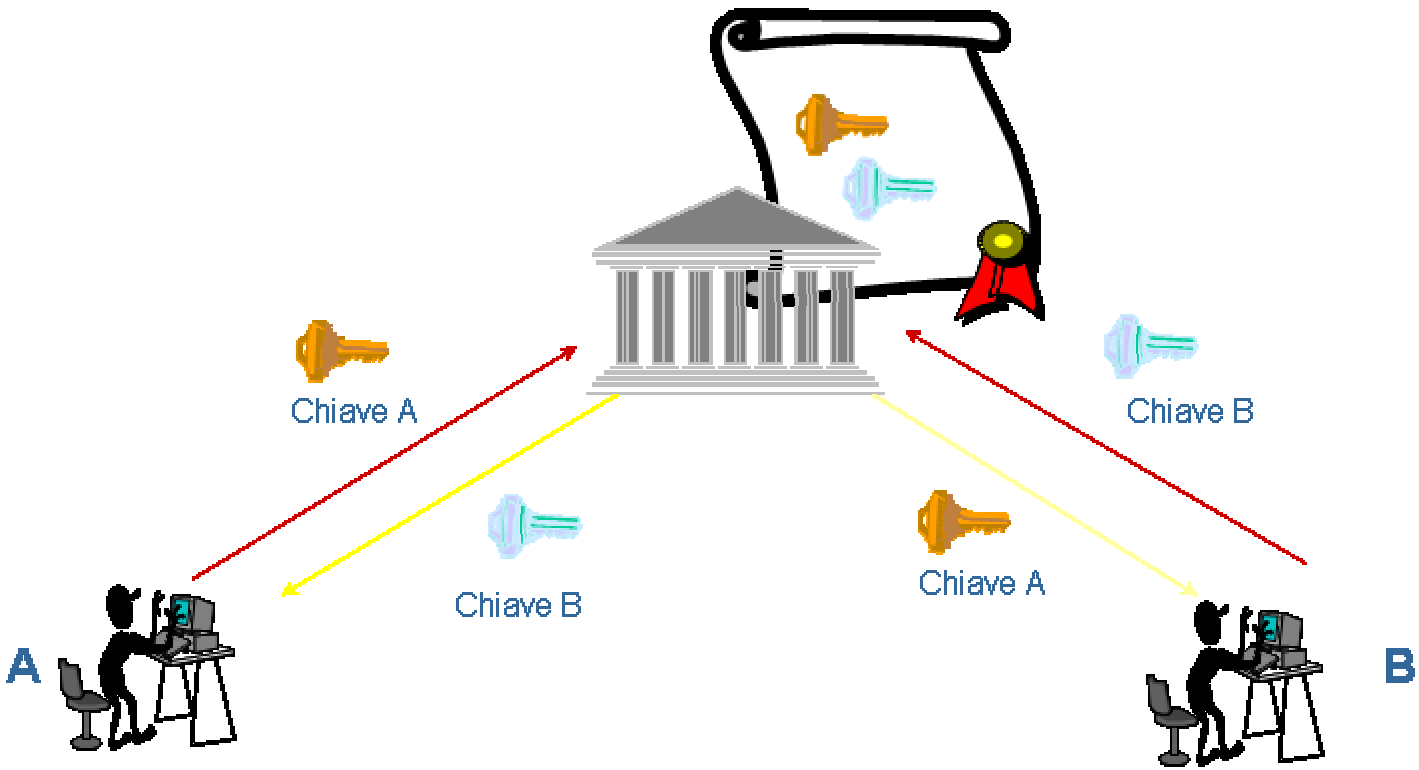
- **Comunicazione sicura tra le parti**
  - Autenticità del mittente
  - Non ripudio
  - Cifratura delle informazioni in transito

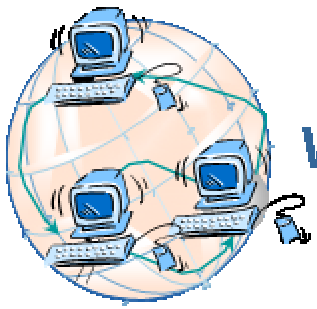
- **Strumento per l'autenticazione forte**
  - Per l'accesso alle postazioni
  - Per l'utilizzo di applicazioni





Il consiglio permanente utilizza la posta sicura con le smart card



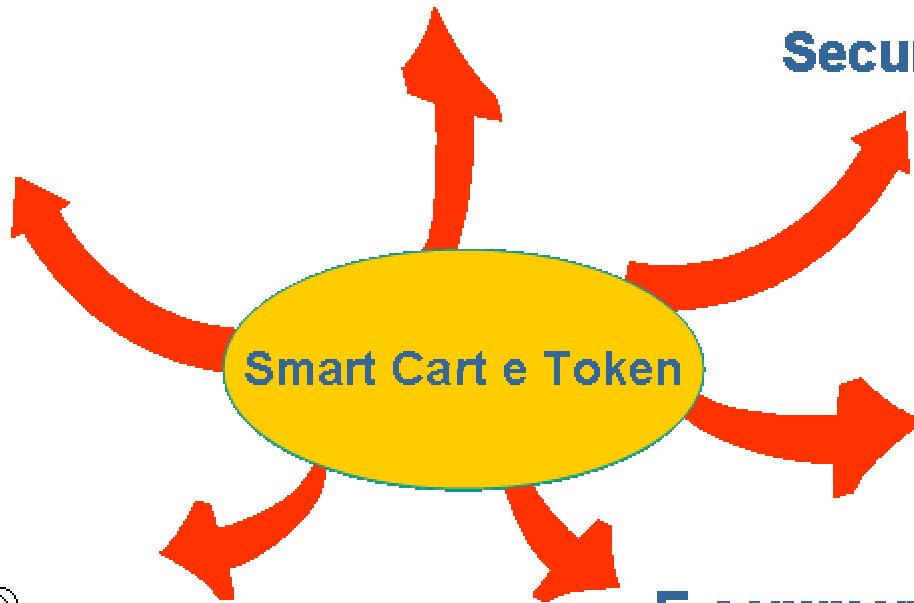


Web

E-mail

Secure Desktop

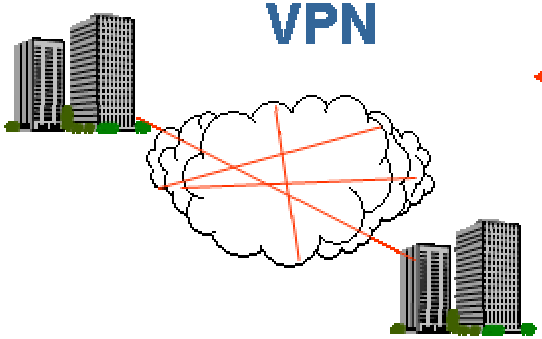
Mobile



Single Sign On

****

VPN



E-commerce