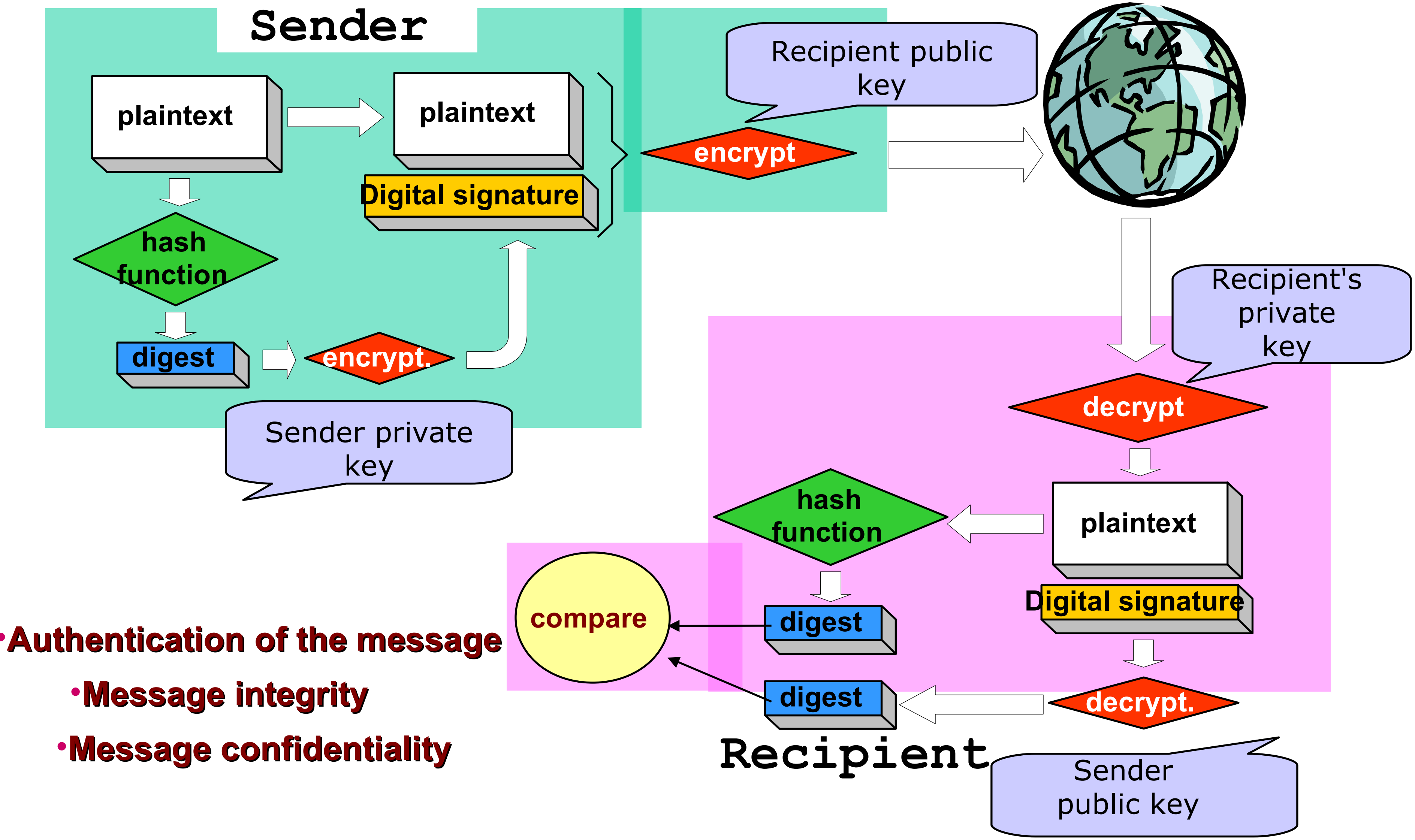
PKI
and
digital signature

Asymmetric crypto usage



- Authentication of the message
  - Message integrity
  - Message confidentiality

A case of identity

- A digital signature ensures that plaintext was authored by someone…
- Not really! It ensures it was encrypted with a certain key… says nothing about “who” is using the key
- Exchange of public keys must be secured (either out-of-band, or otherwise)
- PKI (Public Key Infrastructure) associates keys with identity on a wide scale

What is a PKI

- A PKI uses a trusted third party to associate keys with subjects
- Called a certification authority (CA)
- The CA digitally signs digital certificates, which bind an identity to a public key
- Now we can recognize a number of subjects... provided that we can obtain the public key of the CA (more on this in a few slides)

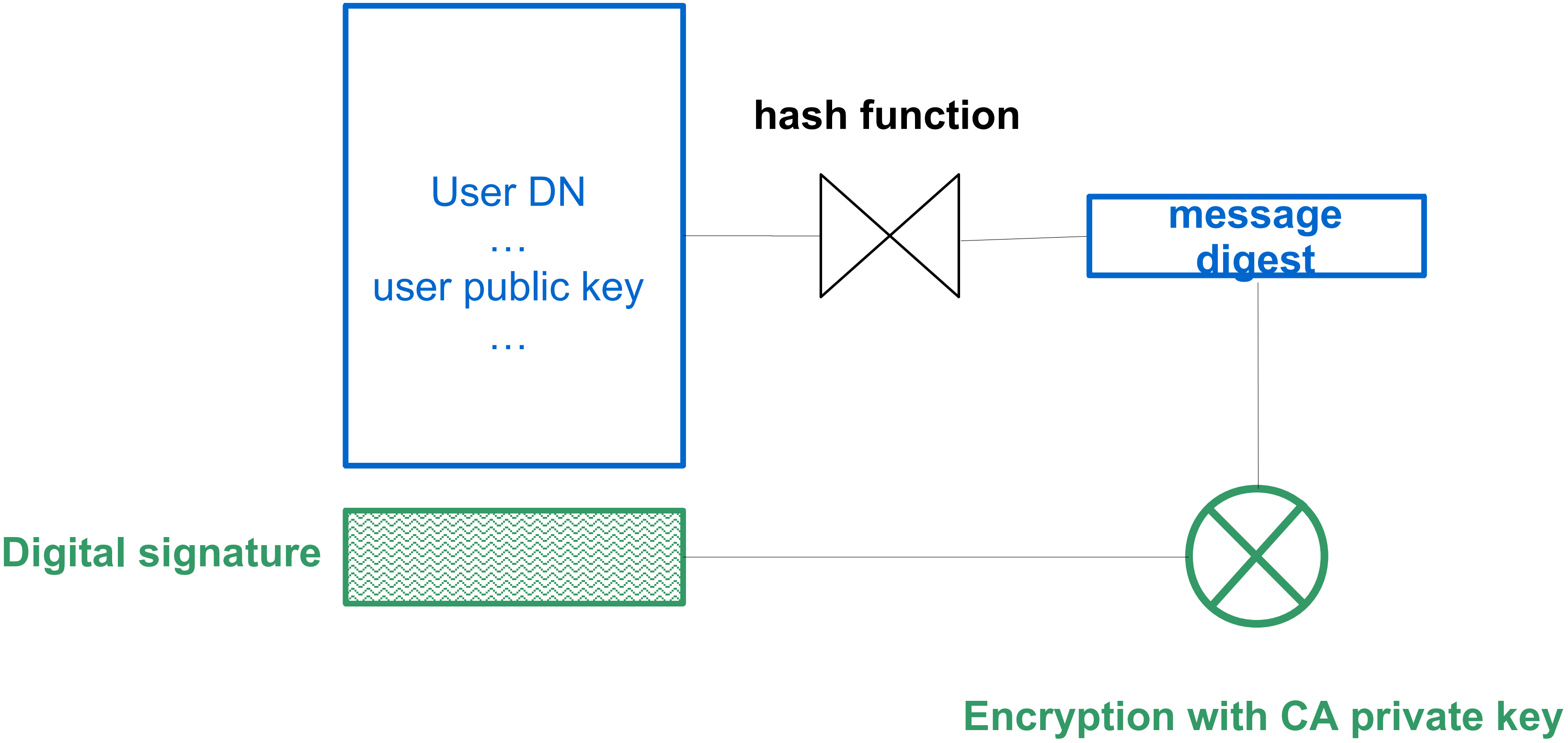
Digital certificate enrollment process

- User proves his identity to the CA (how ?)
- User creates a keypair (public/private) then securely confers the public key to the CA (how ?)
- CA creates a digital certificate, with user public key and ID
- Digital certificate then signed by CA with private key (key management issue!)
- How *could* this possibly fail... ?

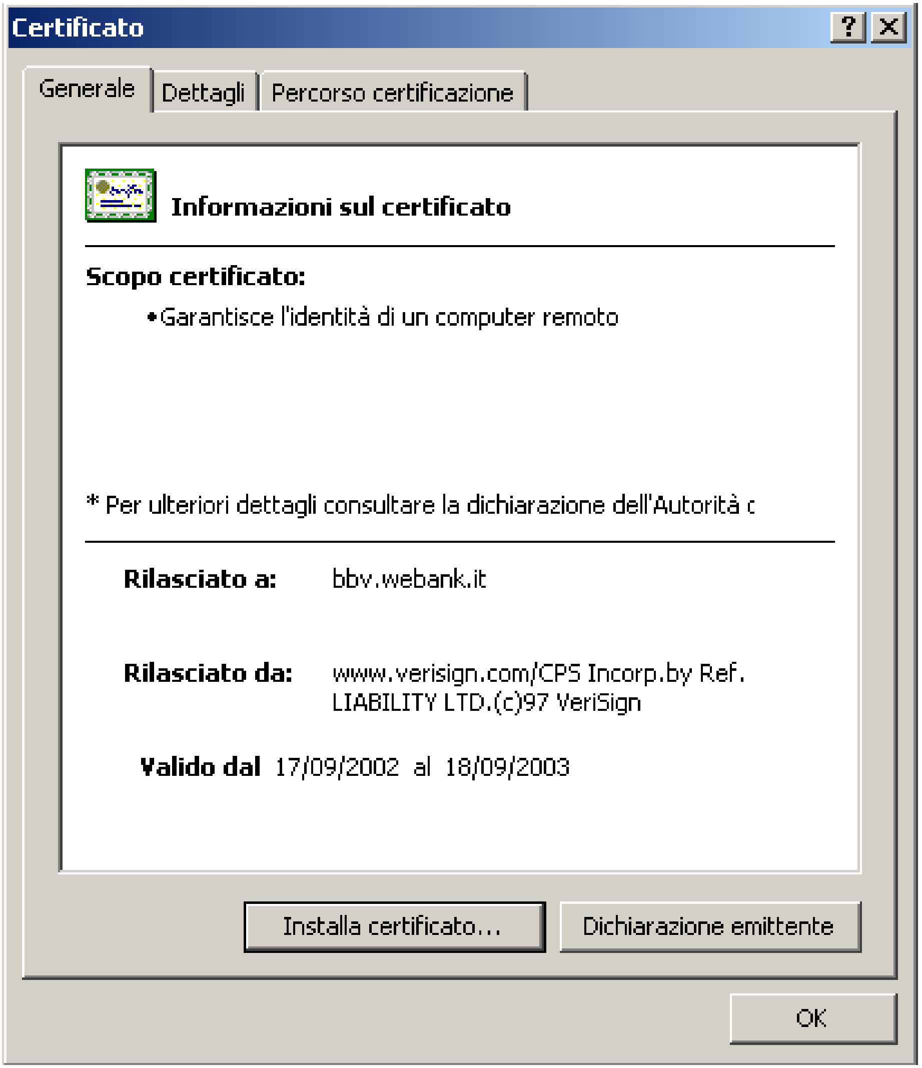
X.509 standard

- Associates a DN (*distinguished name*) to a public key
- X.509 structure certificate
  - Serial number (unique)
  - Public key
  - CA DN
  - Temporal validity
  - Subject DN
  - Cert type and restrictions (server, code signing, ...)
  - CA digital signature

Signature of the certificate



Example of X.509 certificate display



Informazioni sul certificato

Scopo certificato:

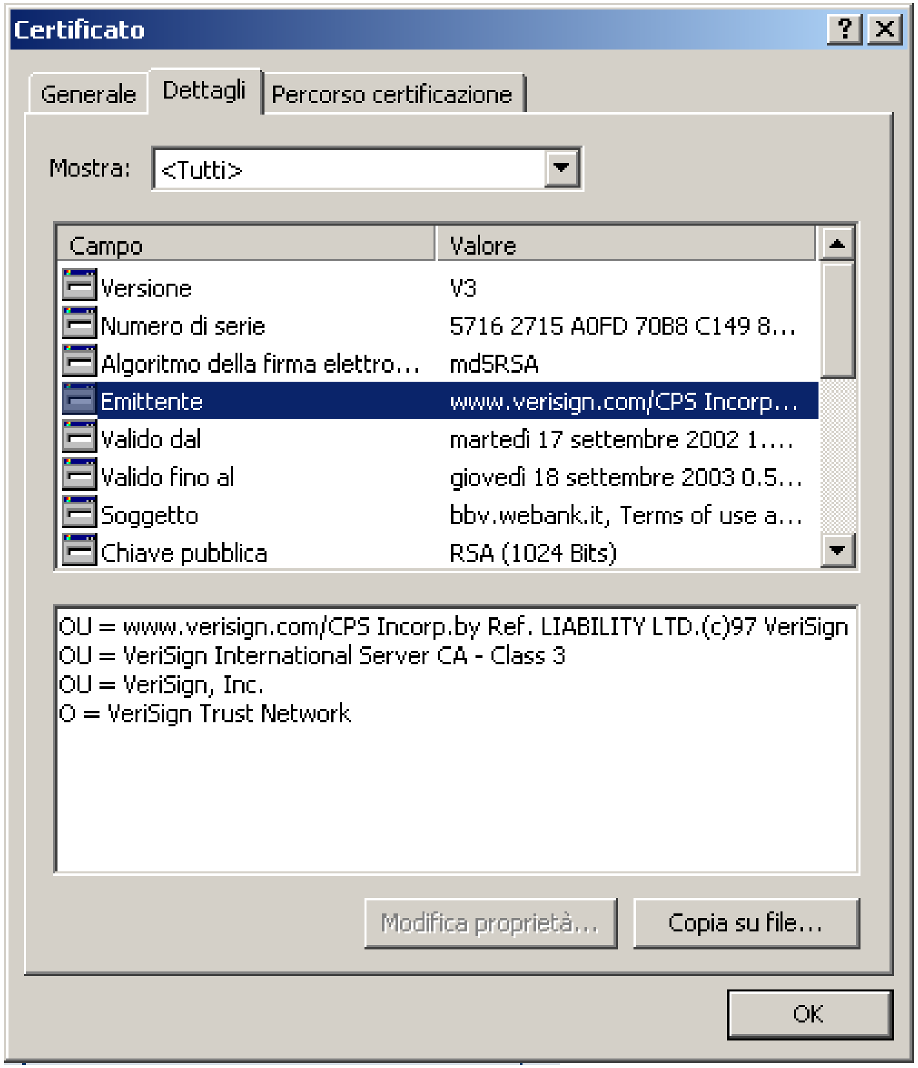
- Garantisce l'identità di un computer remoto

* Per ulteriori dettagli consultare la dichiarazione dell'Autorità c

Rilasciato a: bbv.webank.it

Rilasciato da: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Valido dal 17/09/2002 al 18/09/2003



Mostra: <Tutti>

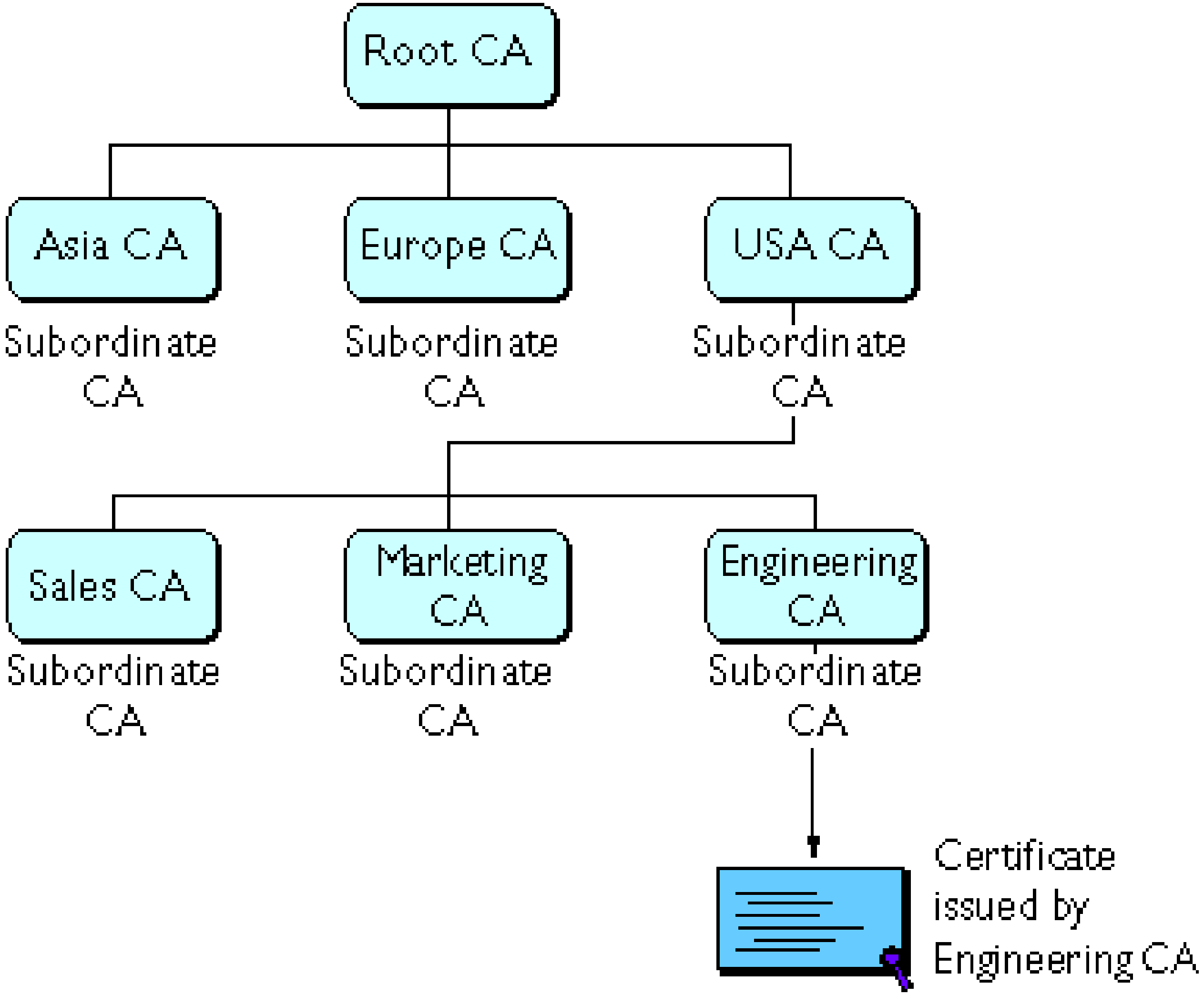
Campo	Valore
Versione	V3
Numero di serie	5716 2715 A0FD 70B8 C149 8...
Algoritmo della firma elettro...	md5RSA
Emittente	www.verisign.com/CPS Incorp...
Valido dal	martedì 17 settembre 2002 1....
Valido fino al	giovedì 18 settembre 2003 0.5...
Soggetto	bbv.webank.it, Terms of use a...
Chiave pubblica	RSA (1024 Bits)

OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
OU = VeriSign International Server CA - Class 3
OU = VeriSign, Inc.
O = VeriSign Trust Network

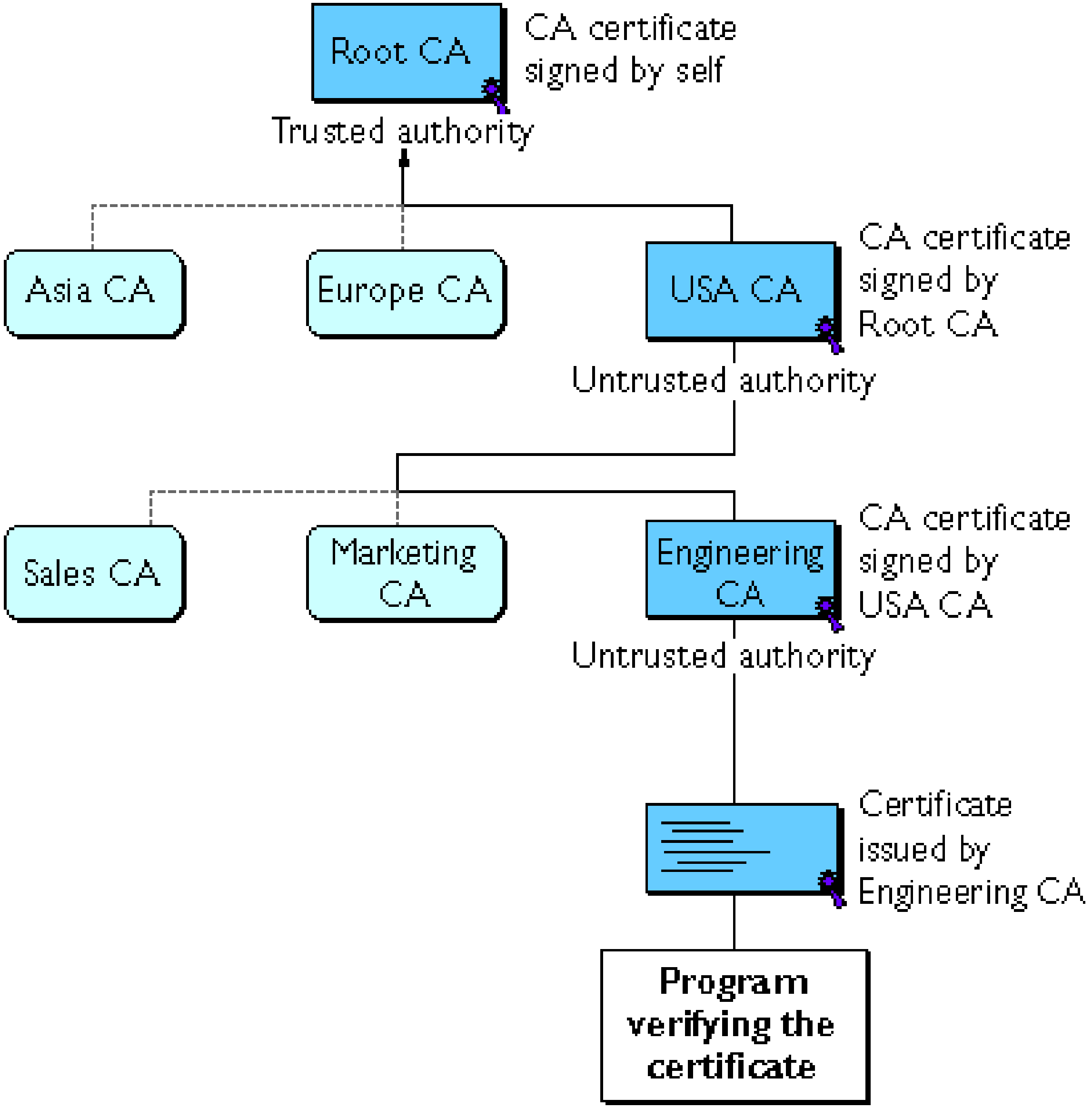
Certificate chains

- *Quis custodiebit custodes?*
- To sign a cert, the CA needs a private key
- The public key... must be in a cert
- Someone else (another CA) signs the cert
- Top-level CA (root CA, source CA, ...) uses a self-signed certificate (which cannot be verified, it's a trusted element)
- How to distribute the trusted element?
  - An authority releases it (the state, a regulator, the organization management)
  - PGP web-of-trust
  - CA already (de facto standard)
- Performance issues?
- Certificate revocation issues (CRL, Certificate Revocation Lists)

Certification Authorities in a hierarchy



Verification of a chain of certificates



Root CA
CA certificate signed by self
Trusted authority
Asia CA
Europe CA
USA CA
CA certificate signed by Root CA
Untrusted authority
Sales CA
Marketing CA
Engineering CA
CA certificate signed by USA CA
Untrusted authority
Certificate issued by Engineering CA
Program verifying the certificate

Verification sequence

- Does the user signature validate the document?
  - Hash verification as we have seen
- Is the used PK the one on the certificate?
  - Simple
- Is the certificate the one of the subject we expect?
  - Problems with omonimous subjects, DN
- Is the certificate validated by the signature of the CA?
  - Validation as we have seen, going back on the certification chain
- Is the root certificate a trusted one?
  - The user needs to be already in possession of the root cert?
- Is the certificate in a CRL?
  - How do we get to the CRL if we are not online?

- Any missing check leads to possible vulnerabilities!

Legal value of digital signatures

- Introduced in Italy with D.P.R. 513/97, and many modifications, in particular when implementing EU regulations
- Original Italian scheme: a single valid scheme
  - CA registered in a Government agency list (AIPA, CNIPA, DigitPA)
  - Strong value as proof
- EU schemes and present day Italian scheme: multiple “levels” of signatures, with different values
- On January a new legislation (the so called “new Digital Administration Code”) introduced so much confusion that this year I will SKIP completely the legal definitions

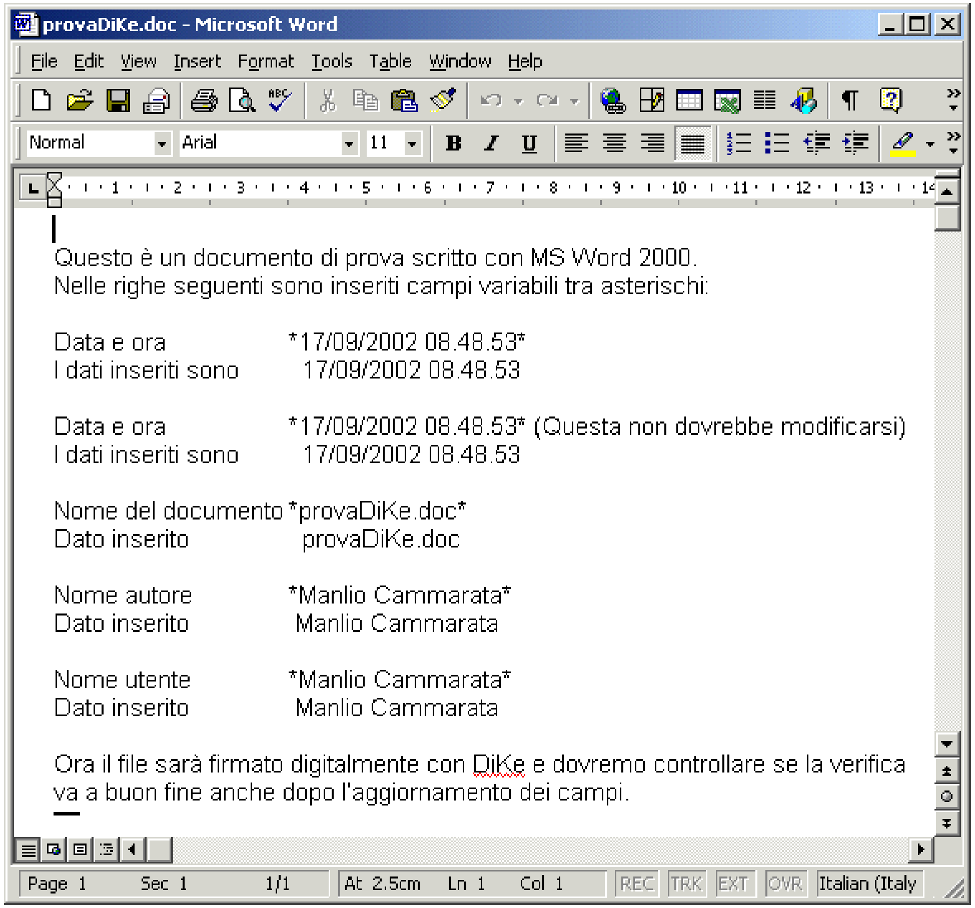
Attacking digital signature applications

- A digital signature is stronger than a handwritten signature
  - Written docs can be modified, signature can be copied... digital signature value tied to content, and cannot be forged unless the algorithm is broken
  - However, digital signature is brittle: if a fake is forged, it cannot be told from the real one
- Is this true?
- Italian signature standards use strong algorithms!
  - No breaks until now
- However, vulnerabilities did emerge
  - Do you remember the “bank vault door in a tent” discussion?

Fields of pain

- Bug notified on 9/9/2002
- The software of several CAs (originally DiKe by Infocamere was the subject of scrutiny) allowed users to sign Word documents with dynamic fields or macros without notice
- A macro does not change the bit sequence of the document, but it changes the visualization
- Examples and stuff are somewhere in my DEI homepage

Results ?


provaDiKe.doc - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Normal
Arial
11
Page 1 Sec 1 1/1 At 2.5cm Ln 1 Col 1 REC TRK EXT OVR Italian (Italy

Questo è un documento di prova scritto con MS Word 2000.
Nelle righe seguenti sono inseriti campi variabili tra asterischi:

Data e ora *17/09/2002 08.48.53*
I dati inseriti sono 17/09/2002 08.48.53

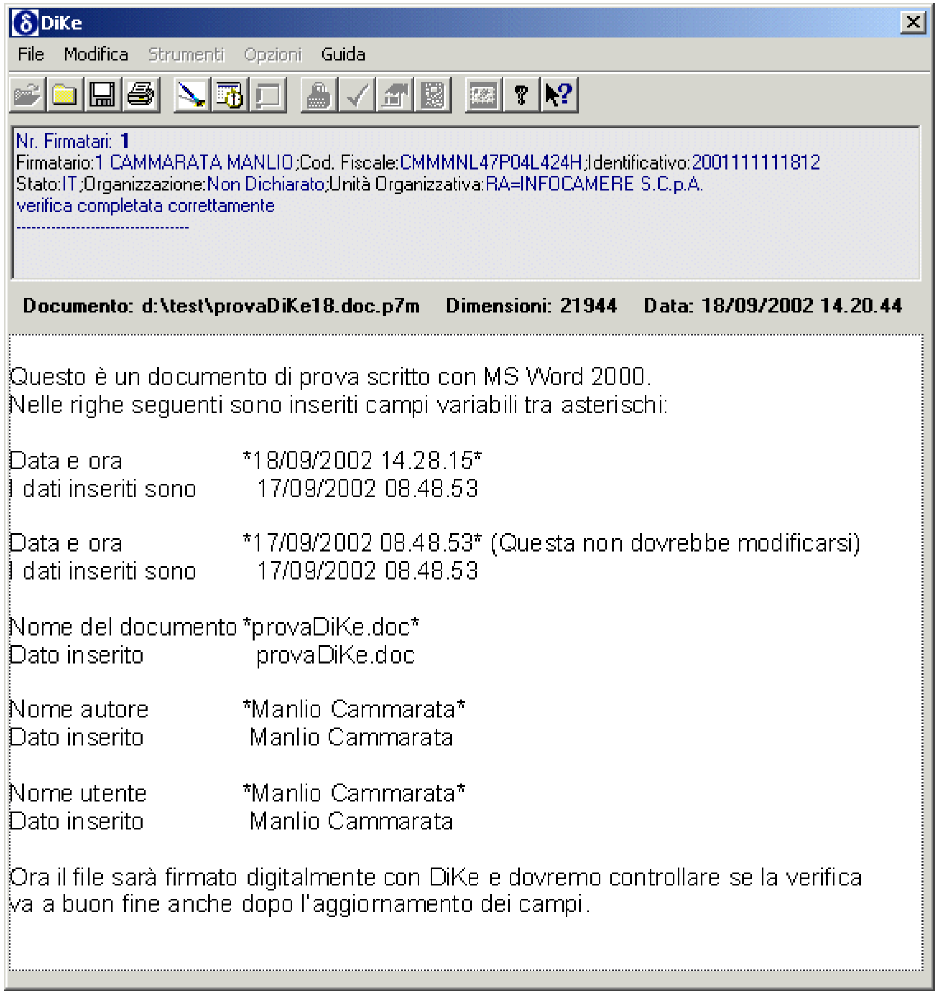
Data e ora *17/09/2002 08.48.53* (Questa non dovrebbe modificarsi)
I dati inseriti sono 17/09/2002 08.48.53

Nome del documento *provaDiKe.doc*
Dato inserito provaDiKe.doc

Nome autore *Manlio Cammarata*
Dato inserito Manlio Cammarata

Nome utente *Manlio Cammarata*
Dato inserito Manlio Cammarata

Ora il file sarà firmato digitalmente con DiKe e dovremo controllare se la verifica va a buon fine anche dopo l'aggiornamento dei campi.



Nr. Firmatari: **1**
Firmatario:1 CAMMARATA MANLIO;Cod. Fiscale:CMMMNL47P04L424H;Identificativo:2001111111812
Stato:IT;Organizzazione:Non Dichiarato;Unità Organizzativa:RA=INFOCAMERE S.C.p.A.
verifica completata correttamente

Documento: d:\test\provaDiKe18.doc.p7m Dimensioni: 21944 Data: 18/09/2002 14.20.44

Questo è un documento di prova scritto con MS Word 2000.
Nelle righe seguenti sono inseriti campi variabili tra asterischi:

Data e ora *18/09/2002 14.28.15*
I dati inseriti sono 17/09/2002 08.48.53

Data e ora *17/09/2002 08.48.53* (Questa non dovrebbe modificarsi)
I dati inseriti sono 17/09/2002 08.48.53

Nome del documento *provaDiKe.doc*
Dato inserito provaDiKe.doc

Nome autore *Manlio Cammarata*
Dato inserito Manlio Cammarata

Nome utente *Manlio Cammarata*
Dato inserito Manlio Cammarata

Ora il file sarà firmato digitalmente con DiKe e dovremo controllare se la verifica va a buon fine anche dopo l'aggiornamento dei campi.

The CA strikes back

- InfoCamere, the vendor, subsequently says that:
  - This is irrelevant, because a directive by AIPA (art. 4 AIPA 51/2000) explicitly states “almeno […] b) la non alterabilità del documento durante le fasi di accesso e conservazione; […] d) l'immutabilità nel tempo del contenuto e della sua struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto“.
  - DiKe, as any other software signs and verifies the content of the document and not its display
  - Office macros cannot be disabled through the API
  - In any case the law does not say anything about this issue (Sacconi, Infocamere)

Is it so?

- At the time, art. 1, T.U. sulla doc. amministrativa: the digital document is *“la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”*. Representation, so what is displayed, actually...
- So the digital signature should not ensure just the integrity of the file but rather of the document
- Actually, even the very first regulation on the subject says (DPCM 8 febbraio 1999 art. 10 c. 1): "Gli strumenti e le procedure utilizzate per la generazione, l’apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, chiaramente e senza ambiguità, i dati a cui la firma si riferisce"
- And the issue has been patched in multiple ways...

Patching

- Microsoft, on Jan 30 2003, completed an Office patch to allow disabling macro fields from the API calls
- Nowadays, DiKe & co. show a big alert whenever you are signing a Word document
- New legislation has explicitly excluded modifiable and scriptable formats. However, PDF has been retained…
- The issue is actually much deeper. Decoders of complex formats should also be validated (think about reading a Word95 document today!)
- A whole research field on “what you see is what you sign” has been completely ignored by lawmakers and vendors

A second bug: Firma&Cifra

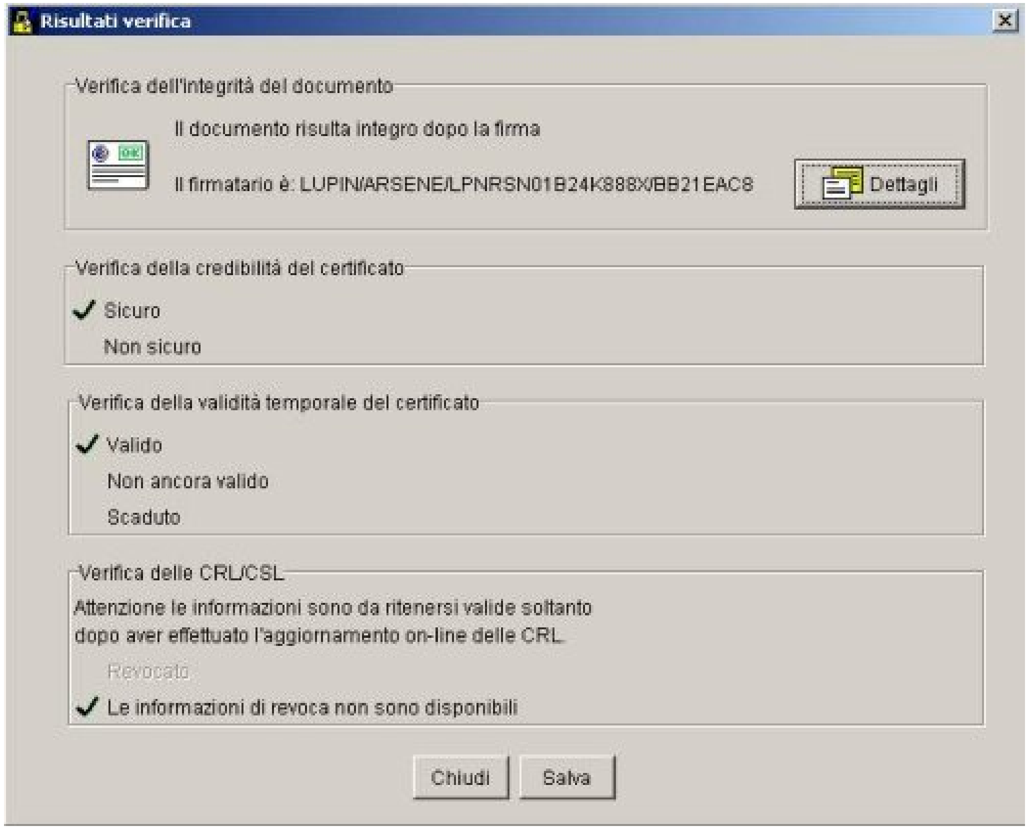
- Firma&Cifra was the digital signature application by PostECom
- Bug found by anonymous on 20/03/2003 http://www.interlex.it/docdigit/sikur159.htm
- Result of the bug: creation and verification of a signature with a fake certificate
- Also in this case: no cryptographic algorithm was broken to perform the show

Bug mechanism

- In order to verify a signature, I need the author cert and the certificate chain
  - Theoretically all available online, but to allow offline verification and to avoid server overload, we distribute everything with the document, in a PKCS#7 standard envelope
- As we know, for the verification we need the root certificate in a secure storage
  - Certificates are usually preinstalled in the software
  - The root cert storage is therefore a critical point!
- Firma&Cifra fatally believes the root certificate in the PKCS#7 envelope, and it even imports it in the secure storage area if it was not there!

Arsène Lupin's signature

- Generate a fake root certificate with the same name as a real one
- Use this to generate a fake user certificate (in our example Arsène Lupin)
- Use Arsène Lupin's certificate to sign theft and burglary confessions
- Add the fake root cert to the PKCS#7 envelope



Verifica dell'integrità del documento

Il documento risulta integro dopo la firma

Il firmatario è: LUPIN/ARSENE/LPNRSN01B24K888X/BB21EAC8

Verifica della credibilitá del certificato

✓ Sicuro

Non sicuro

Verifica della validità temporale del certificato

✓ Valido

Non ancora valido

Scaduto

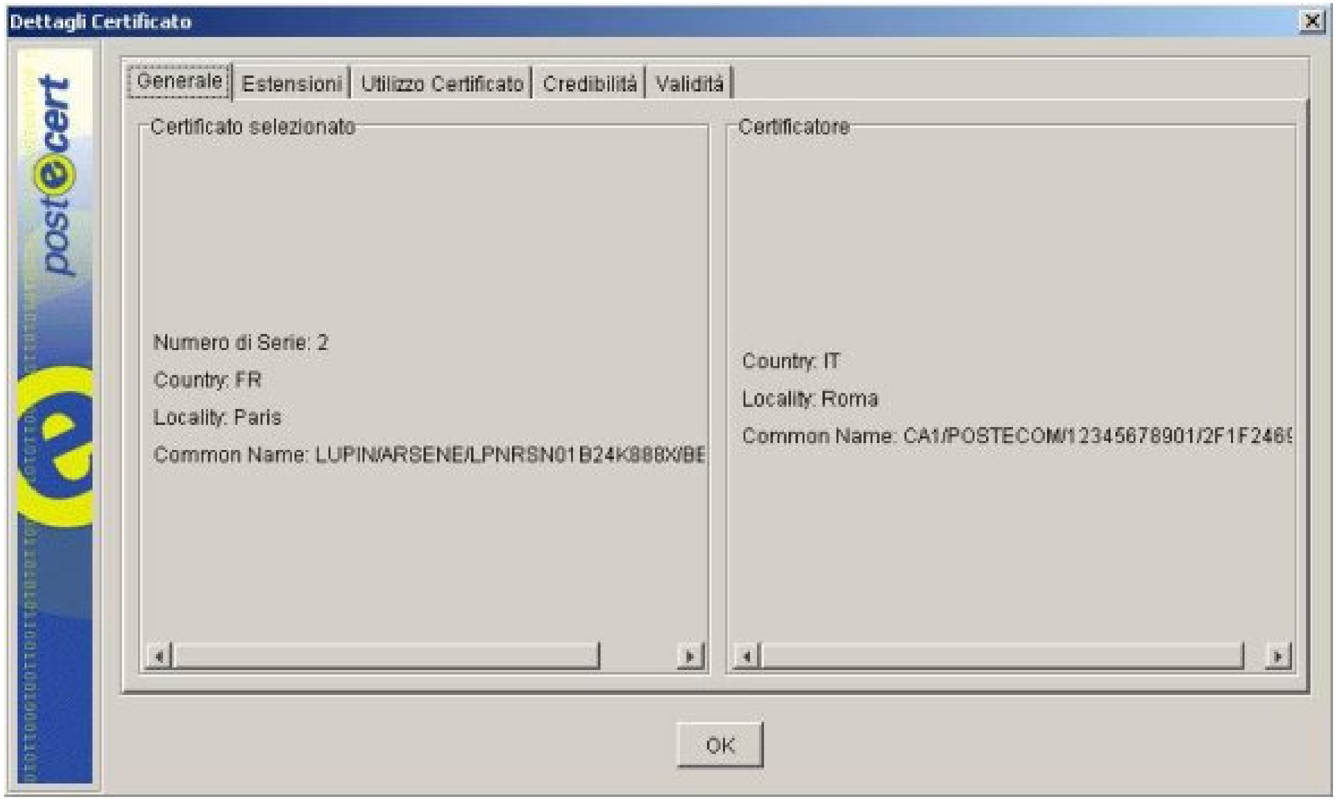
Verifica delle CRL/CSL

Attenzione le informazioni sono da ritenersi valide soltanto dopo aver effettuato l'aggiornamento on-line delle CRL

Revocato

✓ Le informazioni di revoca non sono disponibili

That's it!



Certificato selezionato

Numero di Serie: 2

Country: FR

Locality: Paris

Common Name: LUPIN/ARSENE/LPNRSN01B24K888X/BE

Certificatore

Country: IT

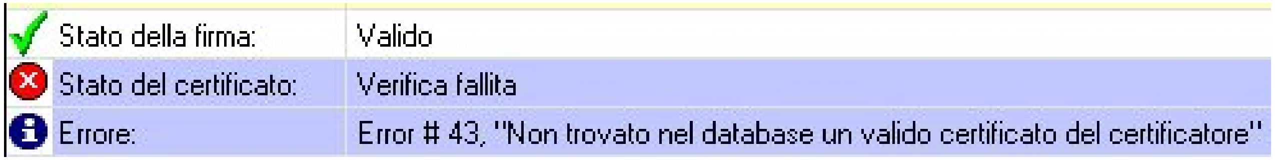
Locality: Roma

Common Name: CA1/POSTECOM/12345678901/2F1F246

- PosteCom says this is “by design” (yep: wrong design, but still design!), and they will require in the future “una più esplicita volontà dell’utente nell’importare un certificato di root”.

Solutions

Any other software says:



✓	Stato della firma:	Valido
✗	Stato del certificato:	Verifica fallita
ℹ	Errore:	Error # 43, "Non trovato nel database un valido certificato del certificatore"

- So the solution is “correct implementation of the software”
- Currently it is called FirmaOK and it's a rewrite, so nothing of this should happen anymore

Host issues

- On May 13 2003 colleagues at UNIMI demonstrated that, if the host machine is trojaned, the security of the signature process is compromised
- Pretty obvious, but think about it: on a trojaned machine... many user machines are trojaned today!
- It is difficult to ensure security for the signature process in such a setting, but it's a need if we wish to distribute digital signatures to a wide number of citizens
- Examples of possible solutions?

Hashing issues

- 2004: several hashing functions partially broken
  - Preimage attack on SHA-0
  - Collisions in MD5
  - Collisions in a weakened SHA-1 (halved rounds)
- 2005: collisions in SHA-1 in 2^{69} instead of 2^{80}
- Collisions on MD5 can be generated with PoC: http://www.stachliu.com/md5coll.c
  - Two certificates with the same hash: http://www.win.tue.nl/~bdeweger/CollidingCertificates/
- Remember: attacks get worse, never better!
- Italian Digital Signature standards do not use endangered algorithms, but:
  - When is one of these attacks acually meaningful?
  - In case, how can we protect the documents?