The digital signature service of the Italian Senate

ECPRD – ICT working group 2009, Italian Parliament

Carlo Marchetti

carlo.marchetti@senato.it

Senato della Repubblica

Topics of the presentation

- Use cases
- System model
- Design principles
- Architectural overview
- Scenarios (screenshots)
- Conclusions

Supported use case(s)

- User R drafts a document D
- D shall be signed by user C, that “owns” a file holder FHc
- C can sign (or refuse to sign) D
- When C signs (or refuses) D, R is notified
- Of course, R could coincide with C, and there can be several Rs, and Cs (each with its own FH)

Typical document workflow steps.

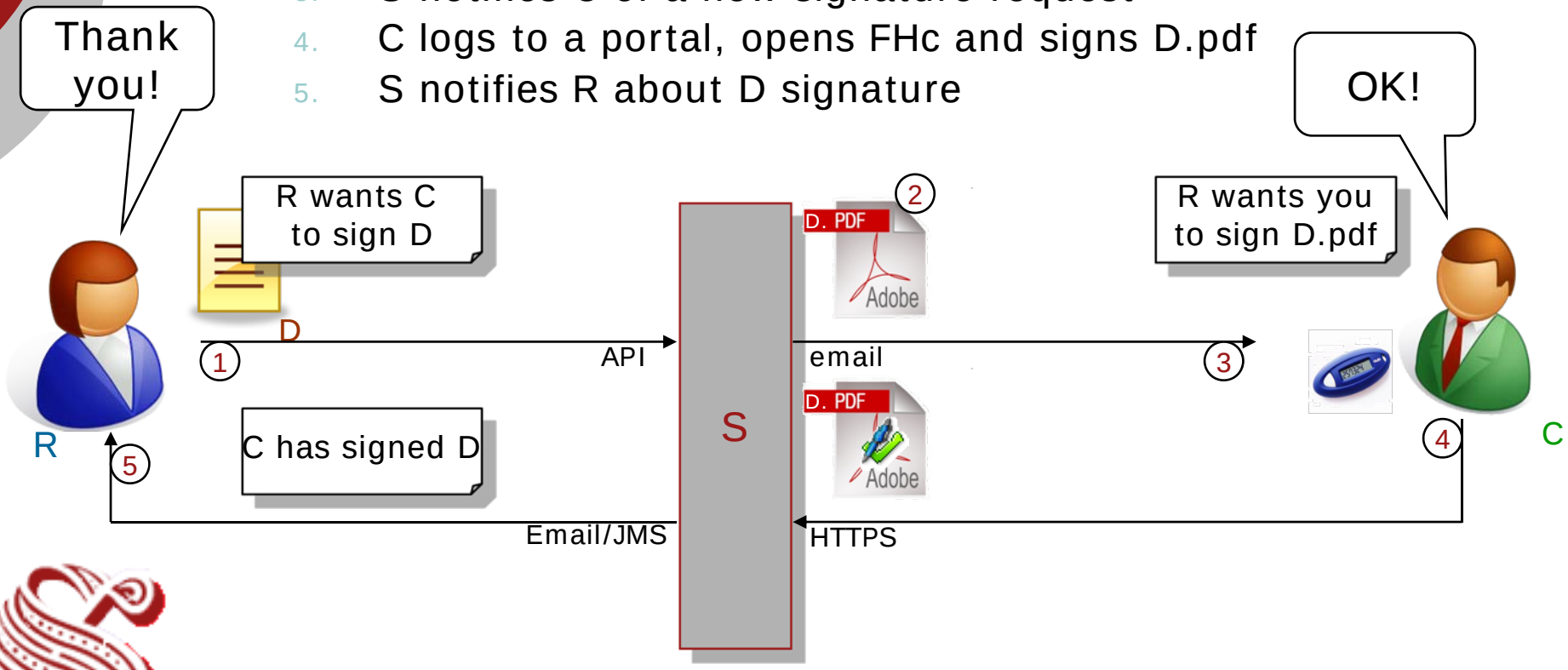
R is an abstraction for D drafters
C is an abstraction D signers

C

C has signed D

System model

- To implement use cases we deploy a system S
  1. S receives from R a "*signature requests*" of D by C
  2. D is converted to D.pdf/A (if necessary) and put in FHc
  3. S notifies C of a new signature request
  4. C logs to a portal, opens FHc and signs D.pdf
  5. S notifies R about D signature

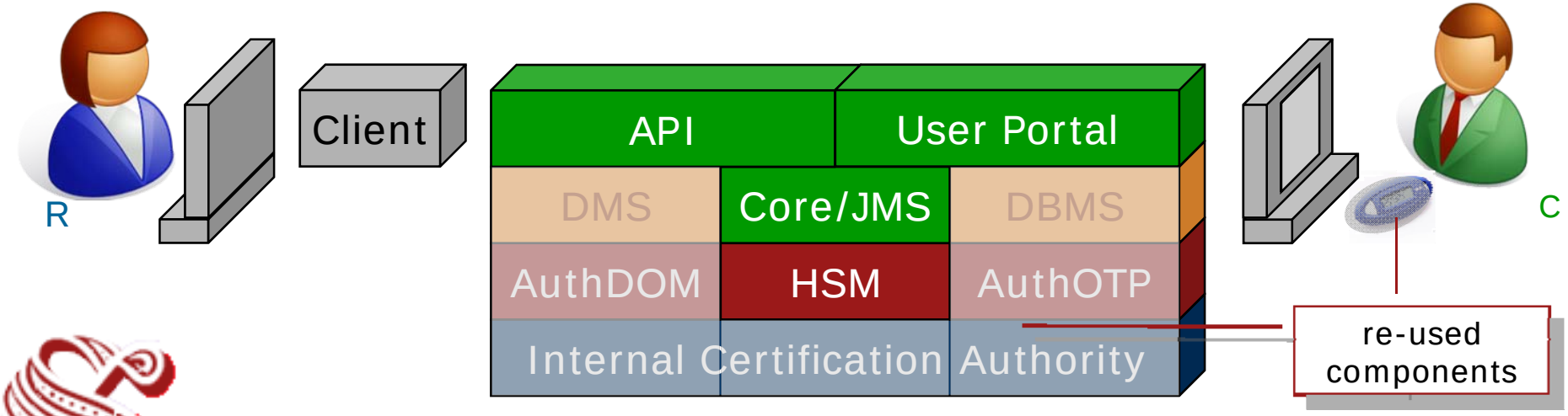


Design principles

- Ease of use for final users
  - simplify user interfaces: use simple metaphors well known to users (show the document, a pen, a graphical signature)
  - minimize necessary devices
  - offer simple document access and verification procedure (pdf)
- Ease of integration with existing systems and document workflows
  - simple API to let external applications use digital signature services
  - pub/sub mechanism (JMS) for forwarding signature events
- Re-use of existing infrastructure (amortize investments)
  - OTP generator and authentication systems
  - CA, DMS, DBMS, and application servers
- Prove and maintain top security levels
  - involve external security auditor

Architectural overview

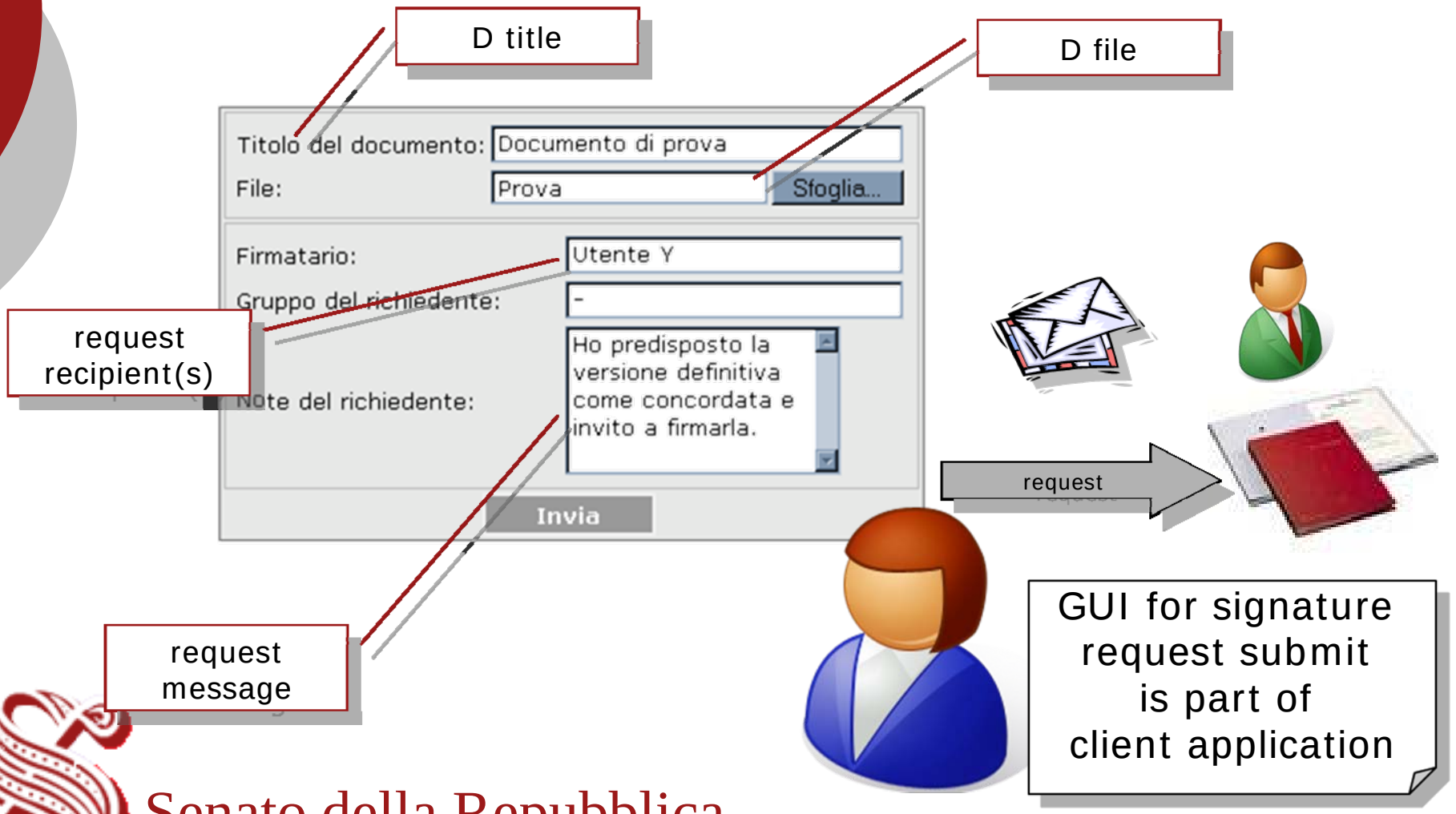
- The system consists of
  - Internal Certification Authority (off-line)
  - HSM for storing keys with API for signing Ds
  - 2 Authentication servers (OTP and domain PWs)
  - DMS and DBMS for storing Ds, signature requests, events
  - Application:
    - Core signature services and JMS queues for event routing
    - Web portal (file holder for Cs)
    - WS-based API for submitting signature requests



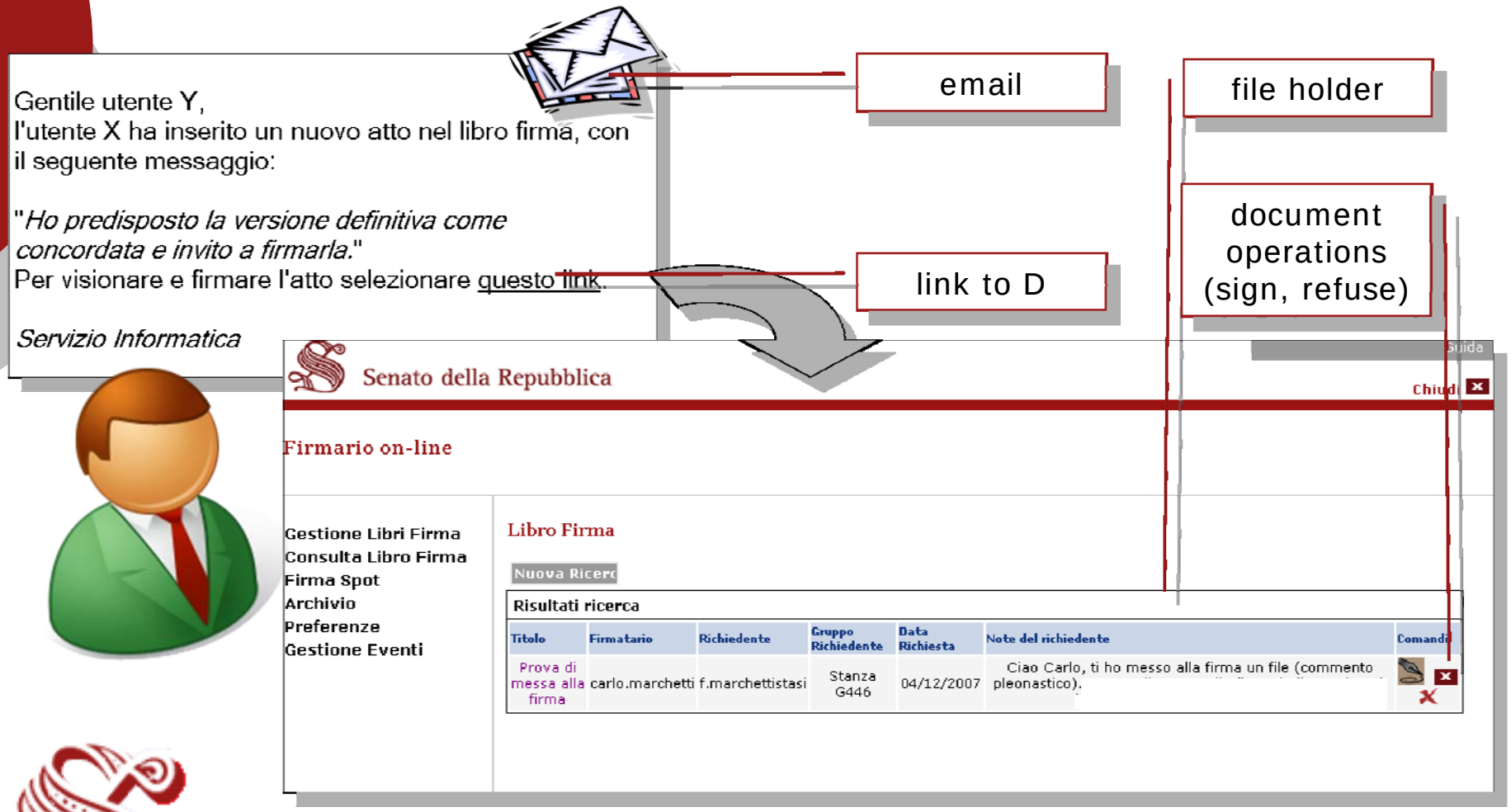
Scenarios and screenshots

1. Signature request submission
2. Signature request notification and access to file holder
3. Signing of a document
4. Search and access the document archive

Screenshots (1)
client request submission interface

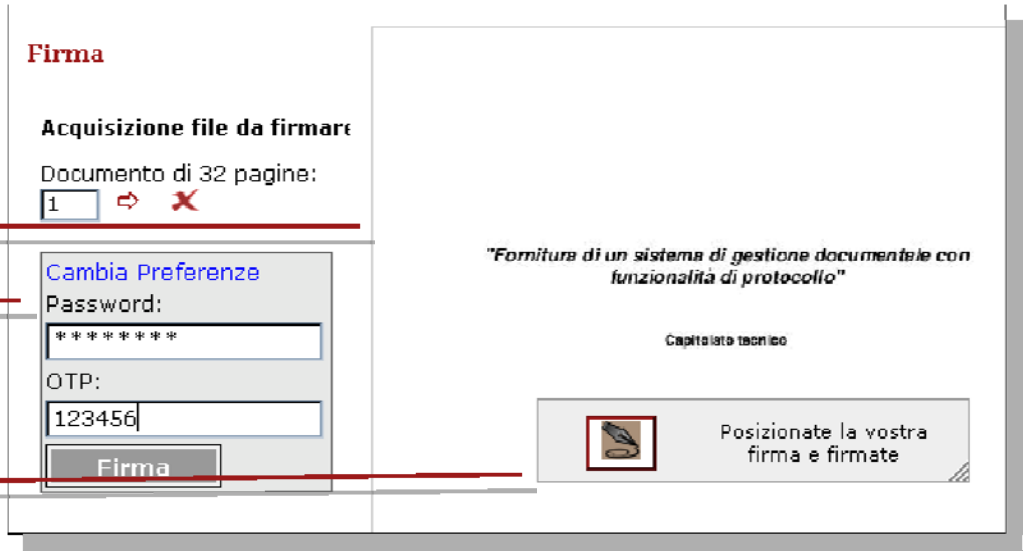


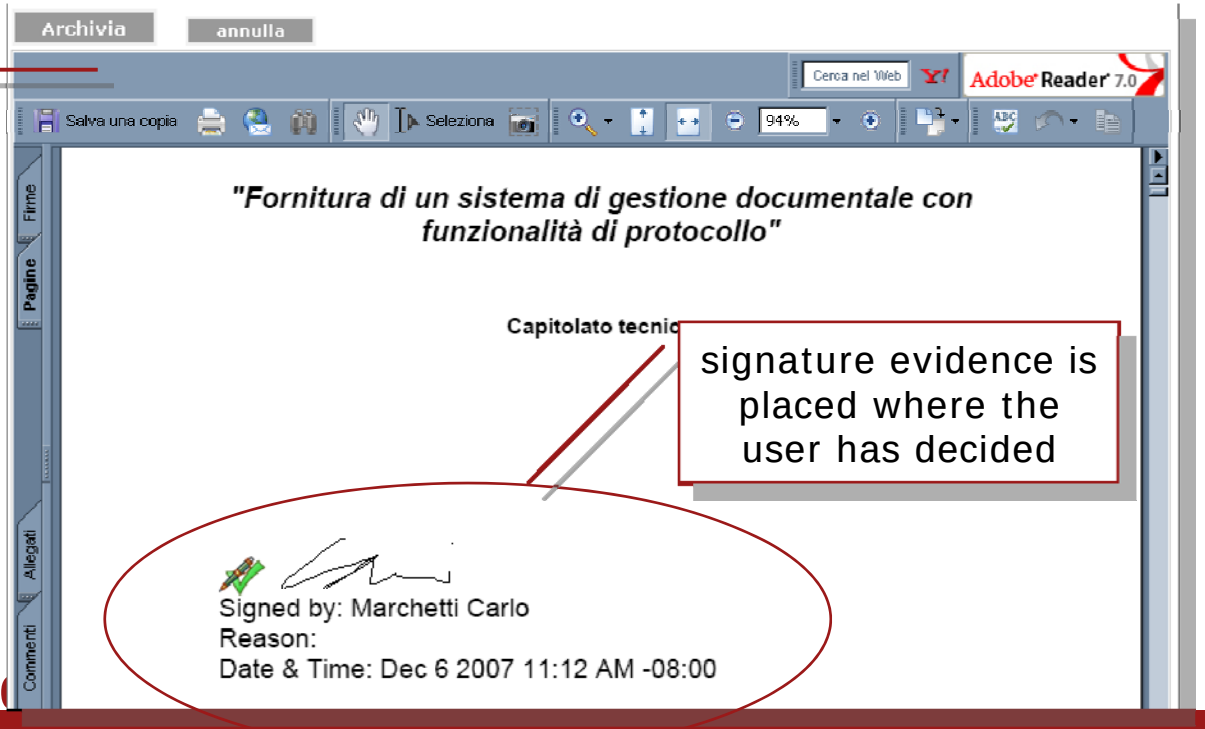
Screenshots (2)
signature request and file holder access



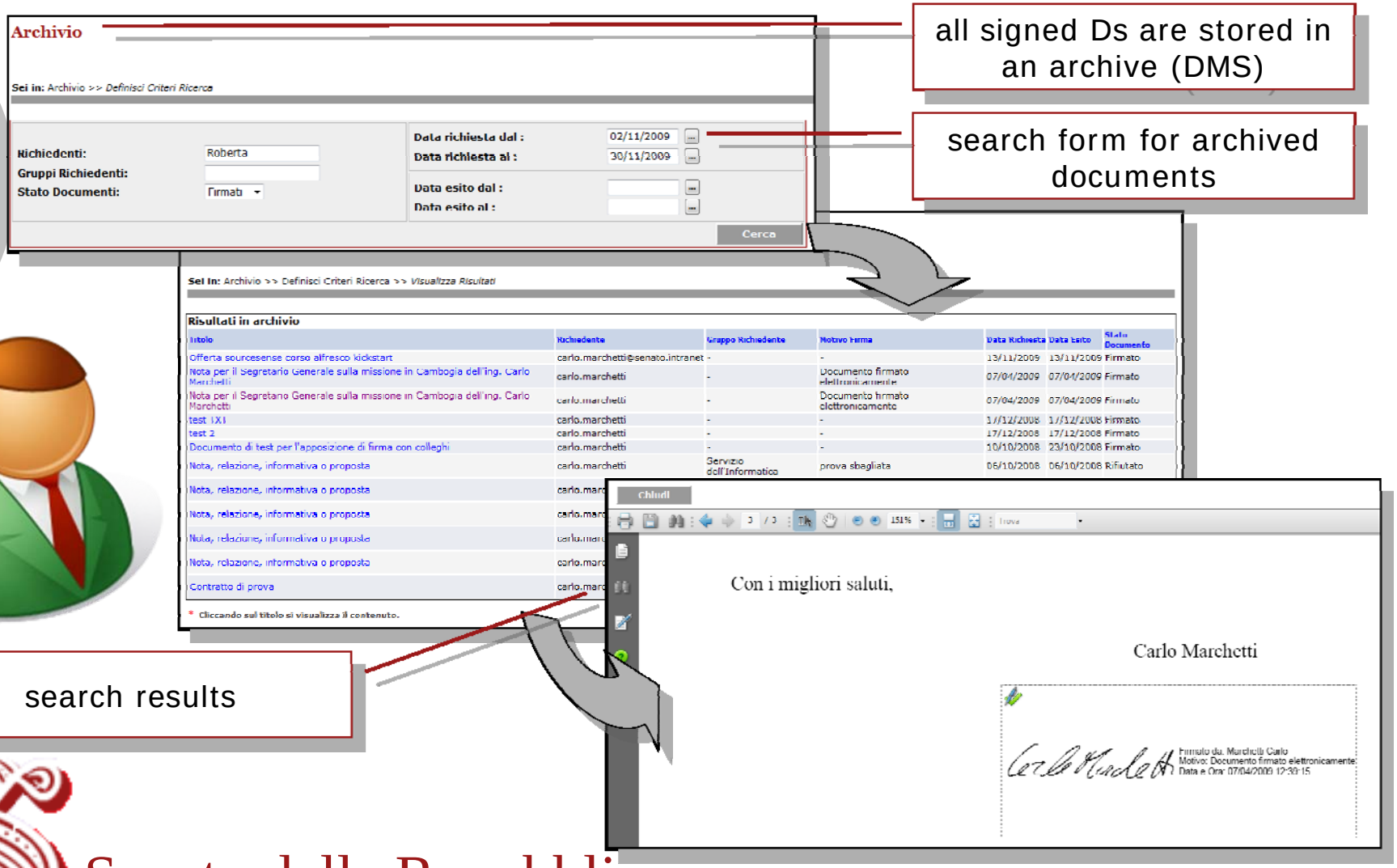
Screenshot (3) signing of a document

- document preview
- double authentication control (OTP and domain PW required)
- graphical signature placement control
- final PDF acceptance and signature check





Screenshot (4)
search and access document archive



all signed Ds are stored in an archive (DMS)

search form for archived documents

search results

Conclusions

- The digital signature service is a centralized and easy-to-integrate system for providing all users with a simple GUI
  - teaching users about the systems requires 20 minutes
  - sw integration requires about 0.5MM
- The system has been integrated in both the legislative (government inspection acts) and the administrative (contracts) areas of the Italian Senate
- User evaluation is ongoing, and the first feedbacks are quite positive
- A security audit has been successfully completed by an external certified auditor

Thank you

Carlo Marchetti