

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

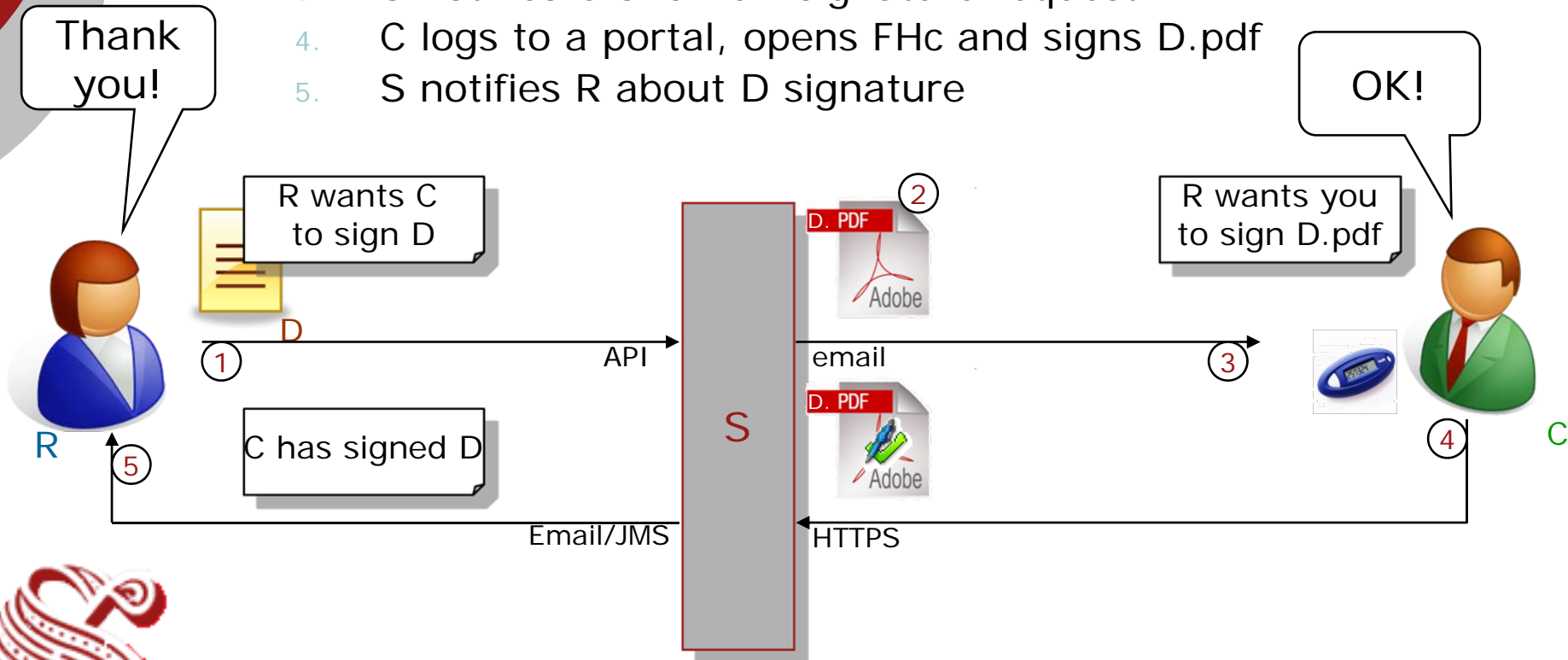


C has signed D



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



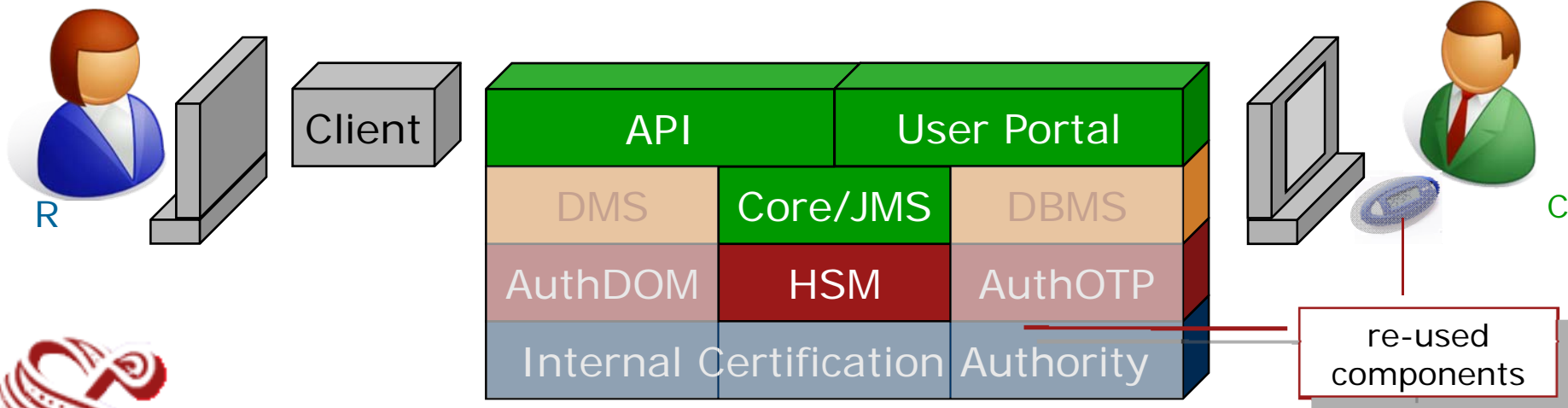
Design principles

- 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



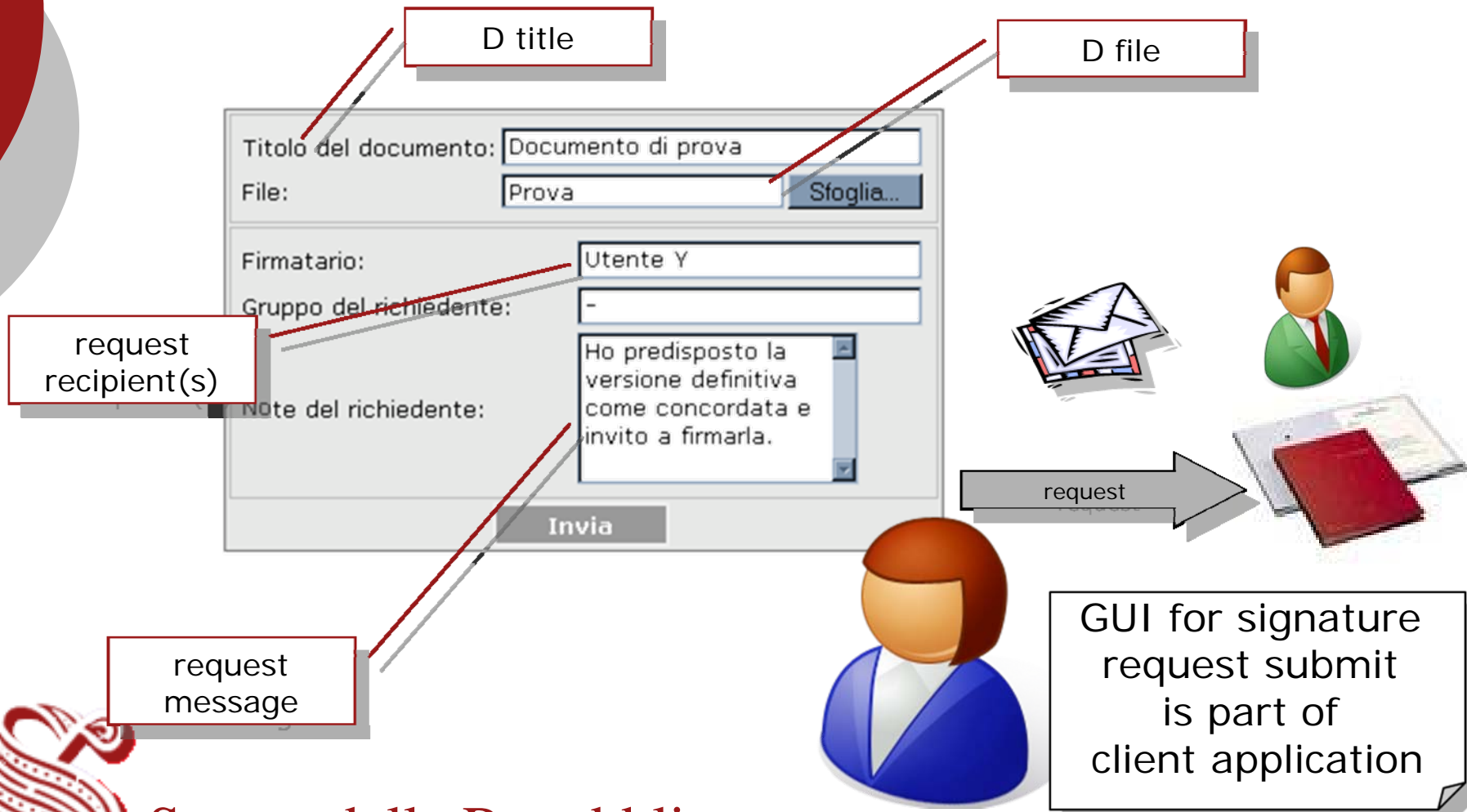
Scenarios and screenshots

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

Gentile utente Y,
l'utente X ha inserito un nuovo atto nel libro firma, con
il seguente messaggio:

*"Ho predisposto la versione definitiva come
concordata e invito a firmarla."*

Per visionare e firmare l'atto selezionare questo link.

Servizio Informatica



email

file holder

document
operations
(sign, refuse)

link to D



 Senato della Repubblica

Chiudi

Firmario on-line

- Gestione Libri Firma
- Consulta Libro Firma
- Firma Spot
- Archivio
- Preferenze
- Gestione Eventi

Libro Firma

Nuova Ricerca

Risultati ricerca

Titolo	Firmatario	Richiedente	Gruppo Richiedente	Data Richiesta	Note del richiedente	Comandi
Prova di messa alla firma	carlo.marchetti	f.marchettitasi	Stanza G446	04/12/2007	Ciao Carlo, ti ho messo alla firma un file (commento pleonastico).	 



Senato della Repubblica

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



Senato della Repubblica

Firma

Acquisizione file da firmare

Documento di 32 pagine:
1

[Cambia Preferenze](#)

Password:

OTP:
123456

Firma

"Fornitura di un sistema di gestione documentale con funzionalità di protocollo"

Capitolato tecnico

Posizionate la vostra firma e firmate

Archivia annulla

Cerca nel Web

Adobe Reader 7.0

Salva una copia

Seleziona

94%

"Fornitura di un sistema di gestione documentale con funzionalità di protocollo"

Capitolato tecnico

signature evidence is placed where the user has decided

Signed by: Marchetti Carlo
Reason:
Date & Time: Dec 6 2007 11:12 AM -08:00

Screenshot (4) search and access document archive

Archivio

Sei in: Archivio >> Definisci Criteri Ricerca

Richiedenti: Roberta
Gruppi Richiedenti:
Stato Documenti: Firmati

Data richiesta dal: 02/11/2009
Data richiesta al: 30/11/2009
Data esito dal:
Data esito al:

Cerca

all signed Ds are stored in an archive (DMS)

search form for archived documents



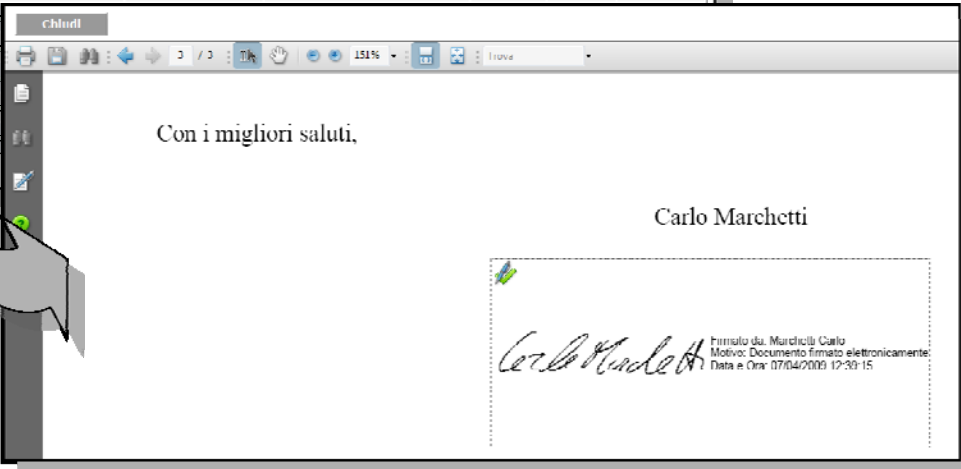
Sei in: Archivio >> Definisci Criteri Ricerca >> Visualizza Risultati

Risultati in archivio

Titolo	Richiedente	Gruppo Richiedente	Motivo tema	Data Richiesta	Data Esito	Stato Documento
Offerta sourcesense corso all'fresco kickstart	carlo.marchetti@senato.intranet	-	-	13/11/2009	13/11/2009	Firmato
Nota per il Segretario Generale sulla missione in Cambogia dell'ing. Carlo Marchetti	carlo.marchetti	-	Documento firmato elettronicamente	07/04/2009	07/04/2009	Firmato
Nota per il Segretario Generale sulla missione in Cambogia dell'ing. Carlo Marchetti	carlo.marchetti	-	Documento firmato elettronicamente	07/04/2009	07/04/2009	Firmato
test 1X1	carlo.marchetti	-	-	17/12/2008	17/12/2008	Firmato
test 2	carlo.marchetti	-	-	17/12/2008	17/12/2008	Firmato
Documento di test per l'apposizione di firma con colleghi	carlo.marchetti	-	-	10/10/2008	23/10/2008	Firmato
Nota, relazione, informativa o proposta	carlo.marchetti	Servizio dell'Informatica	prova sbagliata	06/10/2008	06/10/2008	Rifiutato
Nota, relazione, informativa o proposta	carlo.marchetti	-	-	-	-	-
Nota, relazione, informativa o proposta	carlo.marchetti	-	-	-	-	-
Nota, relazione, informativa o proposta	carlo.marchetti	-	-	-	-	-
Nota, relazione, informativa o proposta	carlo.marchetti	-	-	-	-	-
Contratto di prova	carlo.marchetti	-	-	-	-	-

* Cliccando sul titolo si visualizza il contenuto.

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



Senato della Repubblica