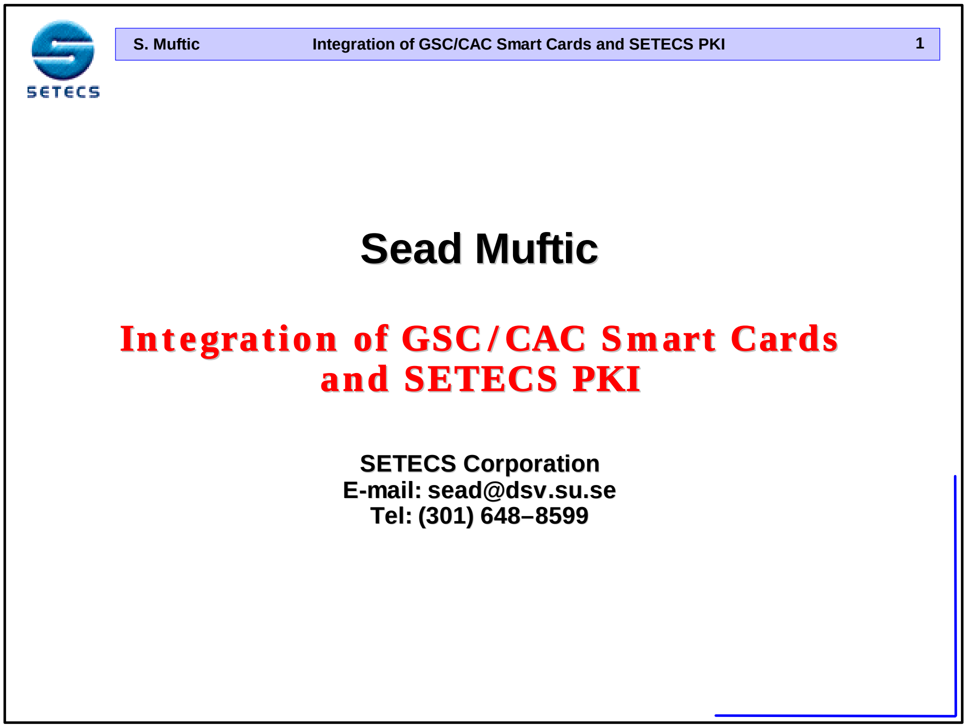
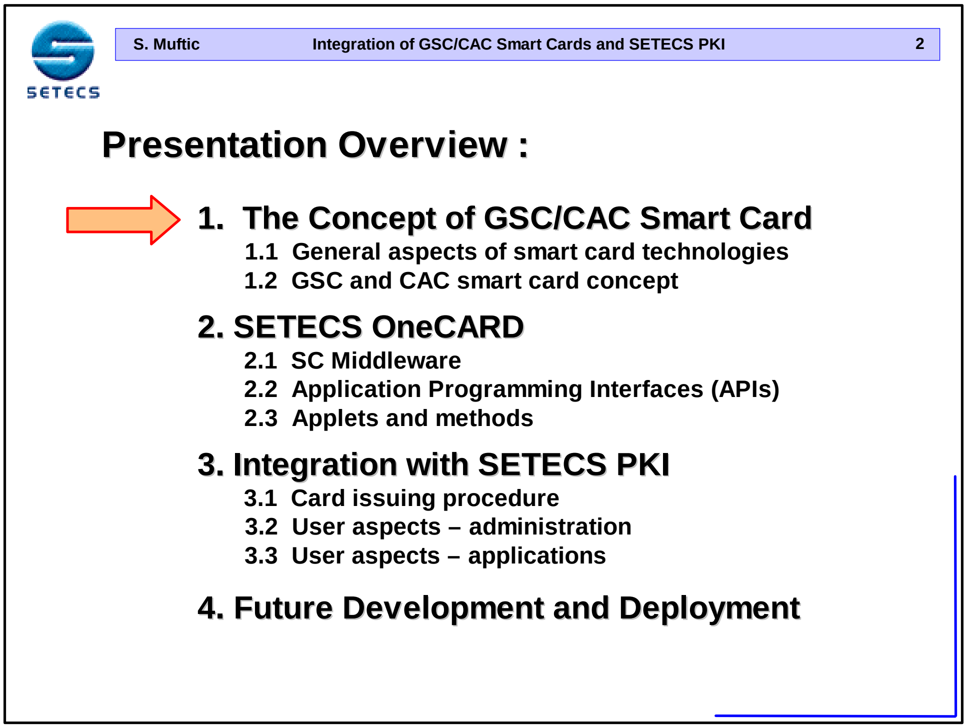


Sead Muftic

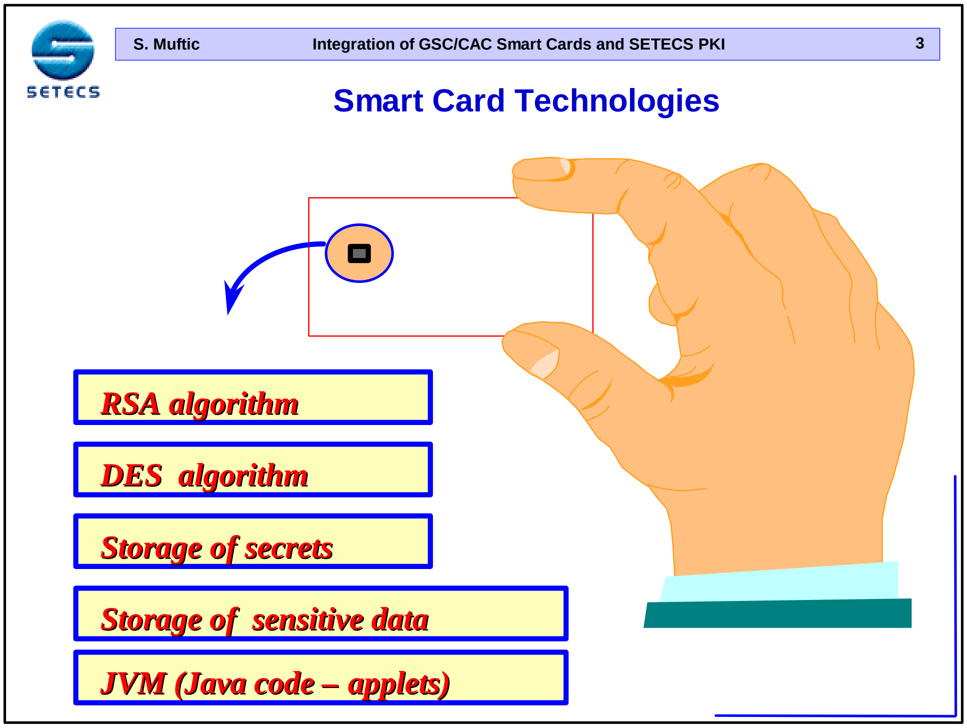
Integration of GSC/CAC Smart Cards and SETECS PKI

SETECS Corporation
E-mail: sead@dsv.su.se
Tel: (301) 648–8599



Presentation Overview :

1. The Concept of GSC/CAC Smart Card
   - 1.1 General aspects of smart card technologies
   - 1.2 GSC and CAC smart card concept
2. SETECS OneCARD
   - 2.1 SC Middleware
   - 2.2 Application Programming Interfaces (APIs)
   - 2.3 Applets and methods
3. Integration with SETECS PKI
   - 3.1 Card issuing procedure
   - 3.2 User aspects – administration
   - 3.3 User aspects – applications
4. Future Development and Deployment



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 3

Smart Card Technologies

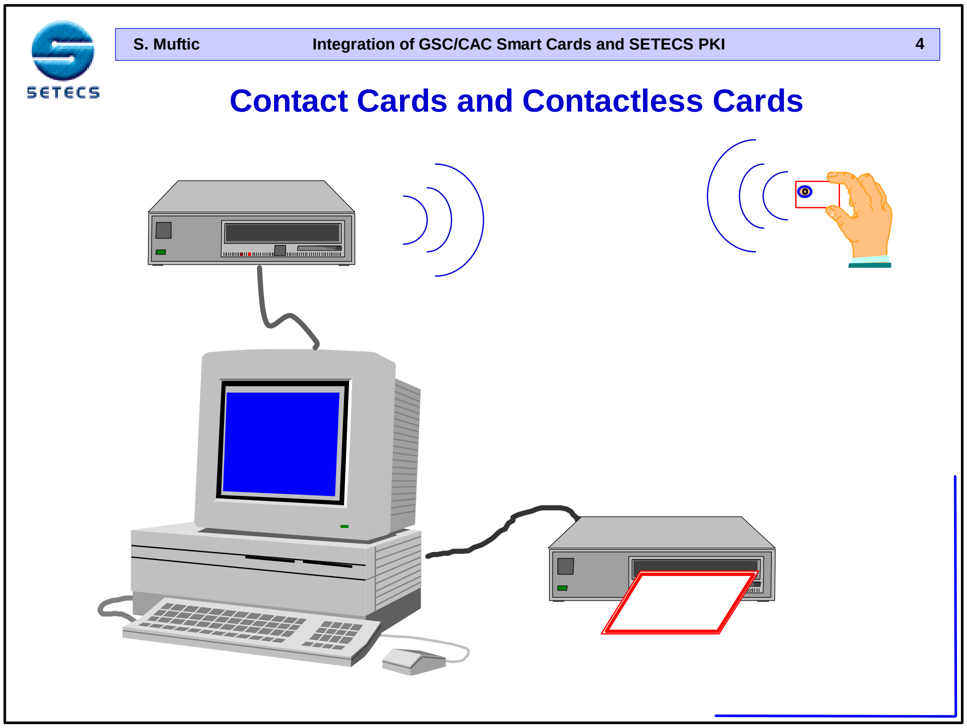
RSA algorithm

DES algorithm

Storage of secrets

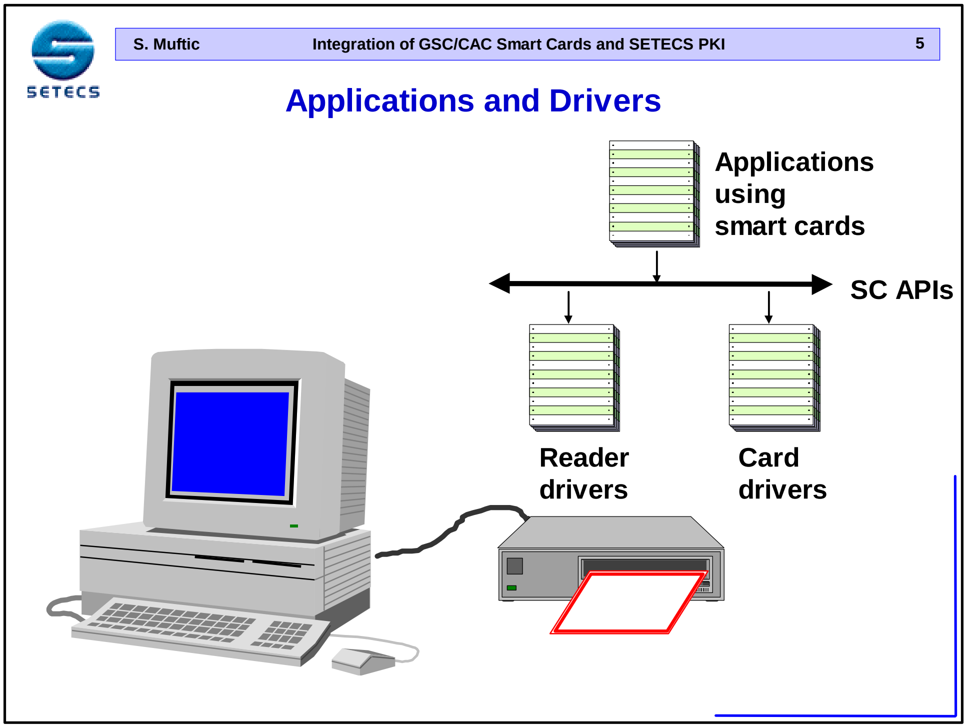
Storage of sensitive data

JVM (Java code – applets)



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 4

Contact Cards and Contactless Cards



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 5

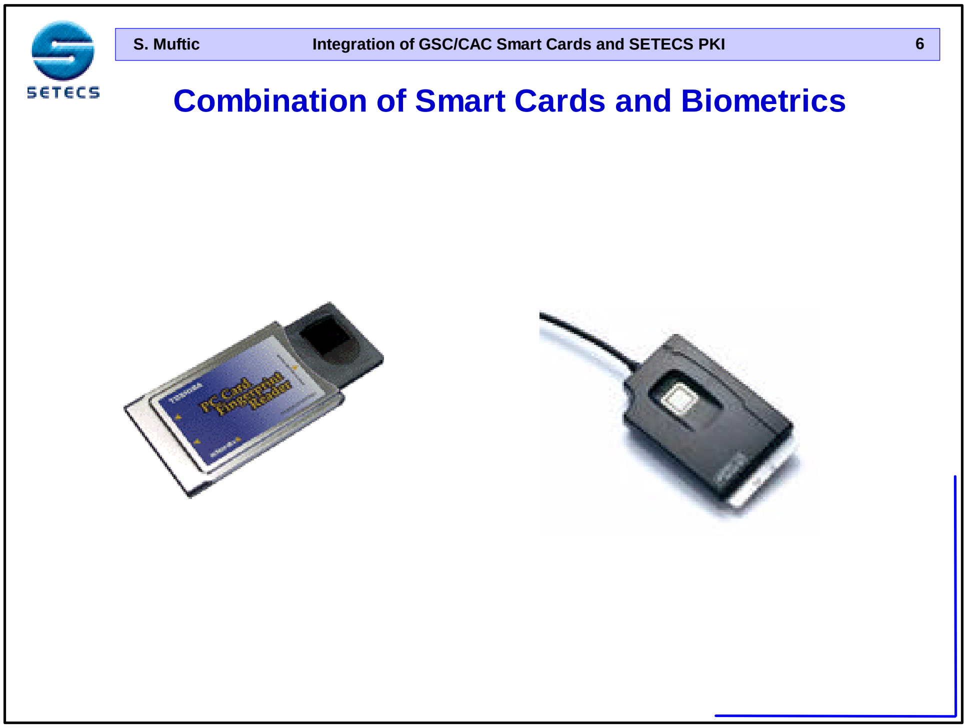
Applications and Drivers

Applications using smart cards

SC APIs

Reader drivers

Card drivers

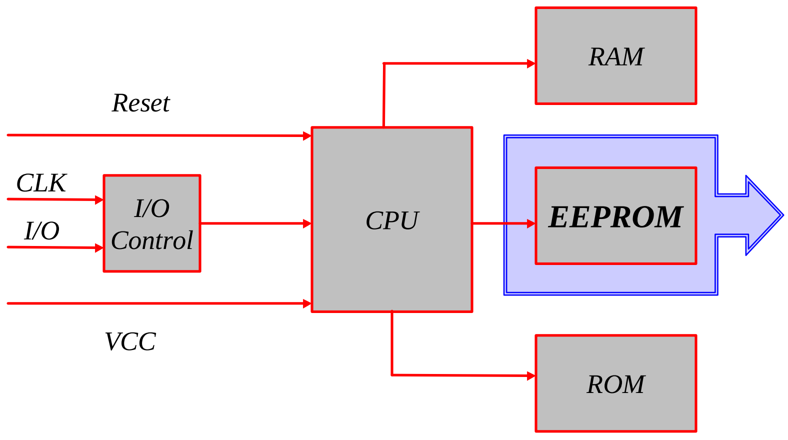


S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 6

Combination of Smart Cards and Biometrics

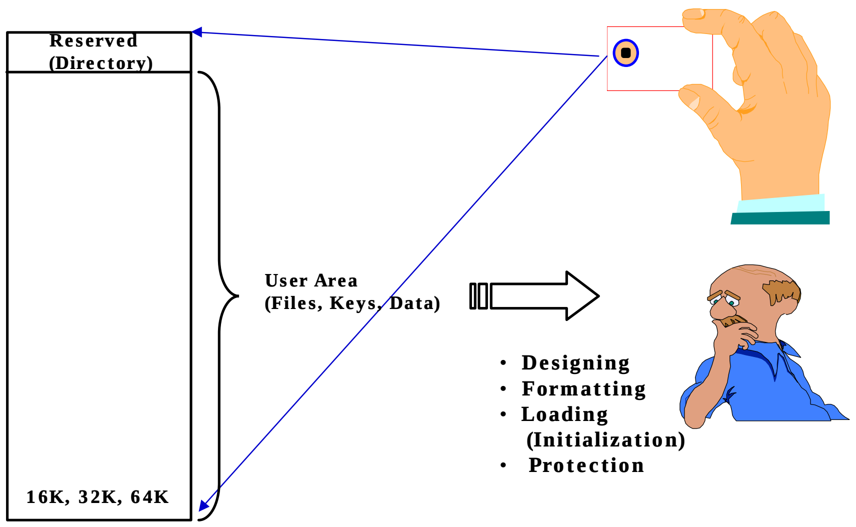
S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 7

Elements of the Smart Card Chip (ICC)



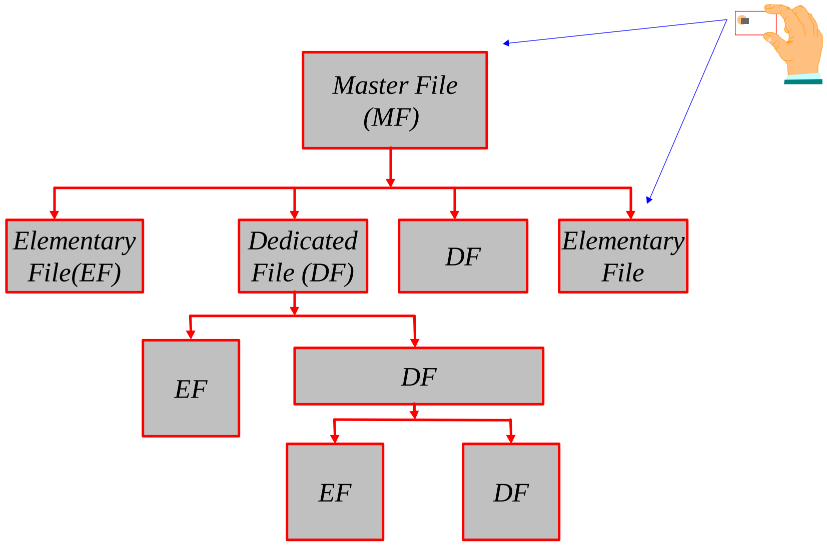
S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 8

Internal Structure of a Smart Card

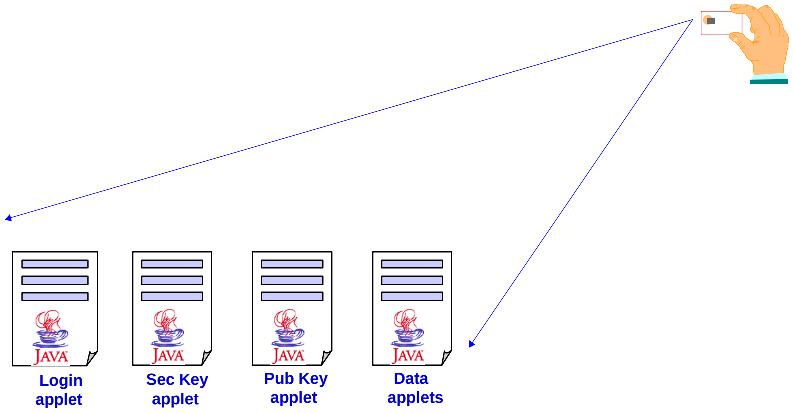


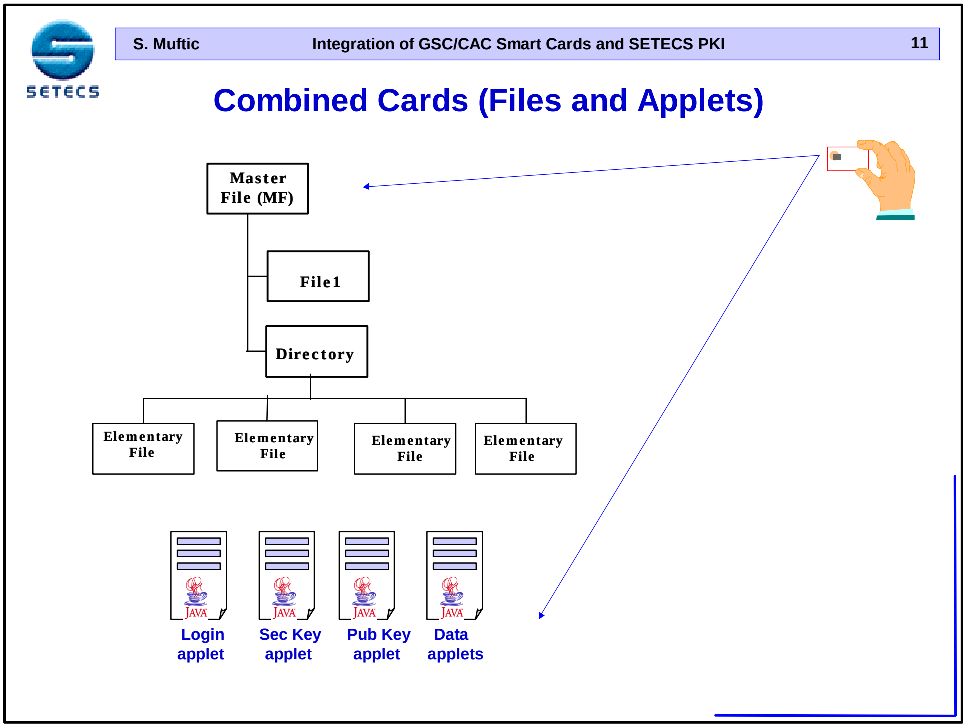
- Designing
- Formatting
- Loading (Initialization)
- Protection

File System Cards (ISO 7816 – 4)



Java Applet Cards (Javacard Framework)





S. Muftic — Integration of GSC/CAC Smart Cards and SETECS PKI — 11

Combined Cards (Files and Applets)

Master File (MF)

File1

Directory

Elementary File

Elementary File

Elementary File

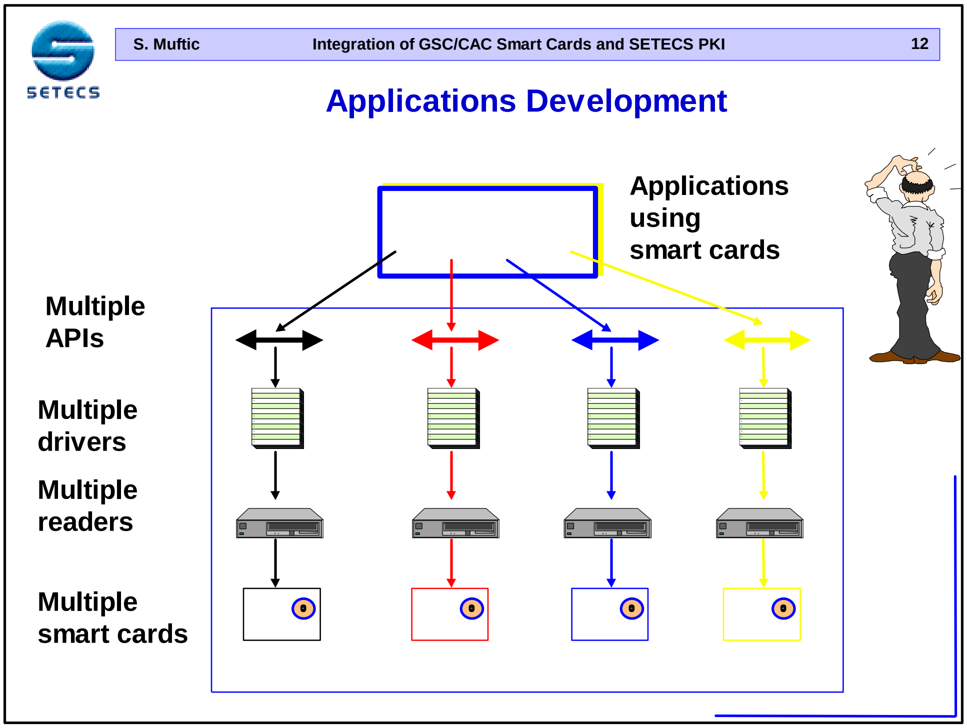
Elementary File

Login applet

Sec Key applet

Pub Key applet

Data applets



S. Muftic — Integration of GSC/CAC Smart Cards and SETECS PKI — 12

Applications Development

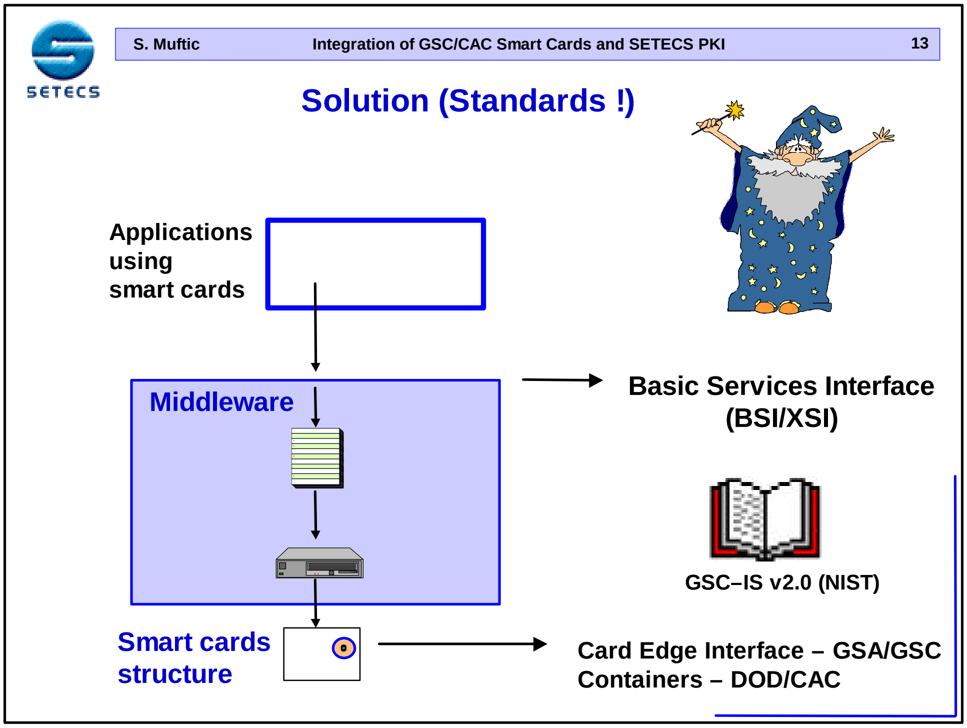
Applications using smart cards

Multiple APIs

Multiple drivers

Multiple readers

Multiple smart cards

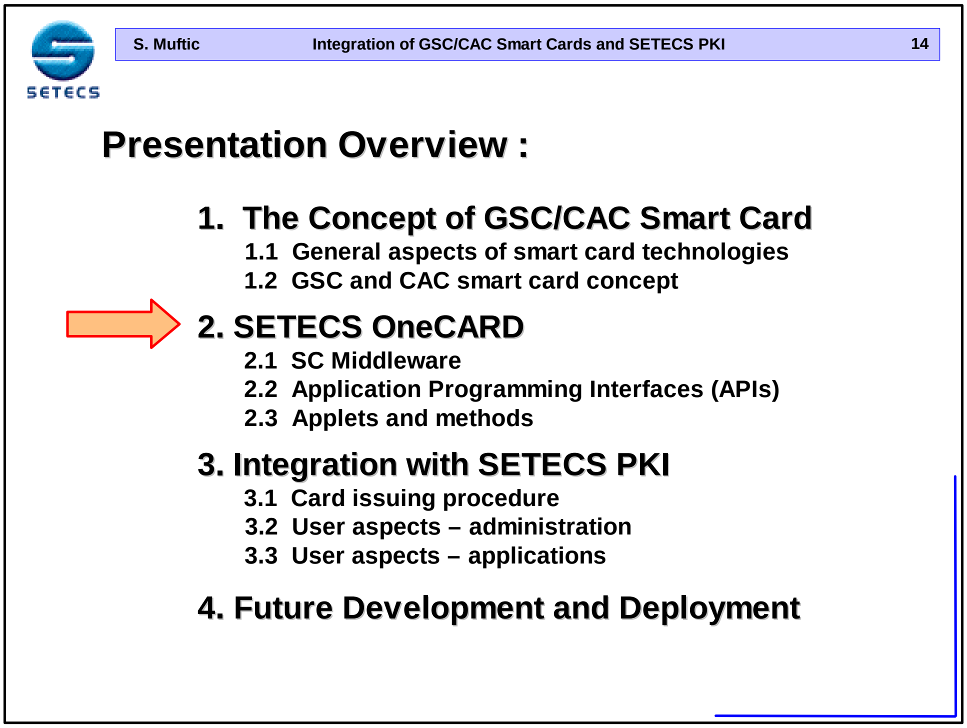


Solution (Standards !)

Basic Services Interface
(BSI/XSI)

GSC–IS v2.0 (NIST)

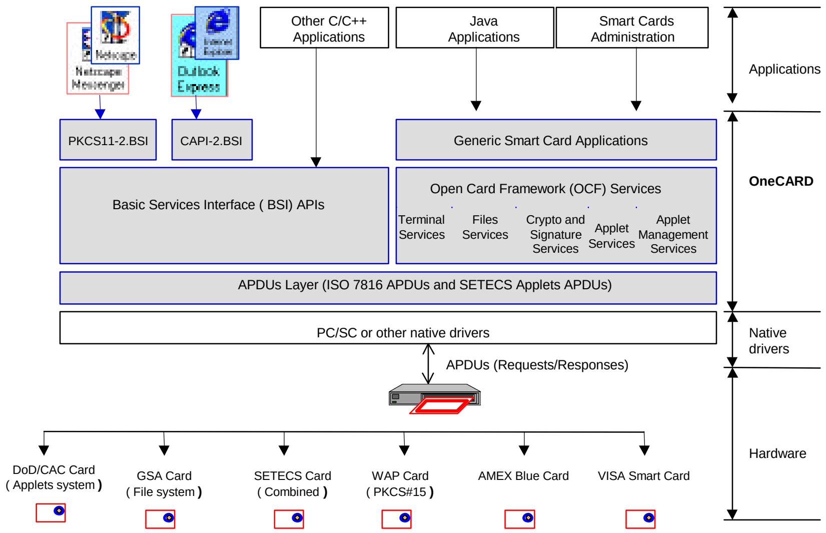
Card Edge Interface – GSA/GSC
Containers – DOD/CAC



Presentation Overview :

1. The Concept of GSC/CAC Smart Card
   - 1.1 General aspects of smart card technologies
   - 1.2 GSC and CAC smart card concept
2. SETECS OneCARD
   - 2.1 SC Middleware
   - 2.2 Application Programming Interfaces (APIs)
   - 2.3 Applets and methods
3. Integration with SETECS PKI
   - 3.1 Card issuing procedure
   - 3.2 User aspects – administration
   - 3.3 User aspects – applications
4. Future Development and Deployment

SETECS *OneCARD* – Middleware


Netscape
Netscape Messenger
Outlook Express
Internet Explorer
Other C/C++ Applications
Java Applications
Smart Cards Administration
Applications
PKCS11-2.BSI
CAPI-2.BSI
Generic Smart Card Applications
OneCARD
Basic Services Interface (BSI) APIs
Open Card Framework (OCF) Services
Terminal Services
Files Services
Crypto and Signature Services
Applet Services
Applet Management Services
APDUs Layer (ISO 7816 APDUs and SETECS Applets APDUs)
PC/SC or other native drivers
Native drivers
APDUs (Requests/Responses)
Hardware
DoD/CAC Card (Applets system)
GSA Card (File system)
SETECS Card (Combined)
WAP Card (PKCS#15)
AMEX Blue Card
VISA Smart Card

Application Programming Interfaces (BSI APIs)

Generic Container Provider

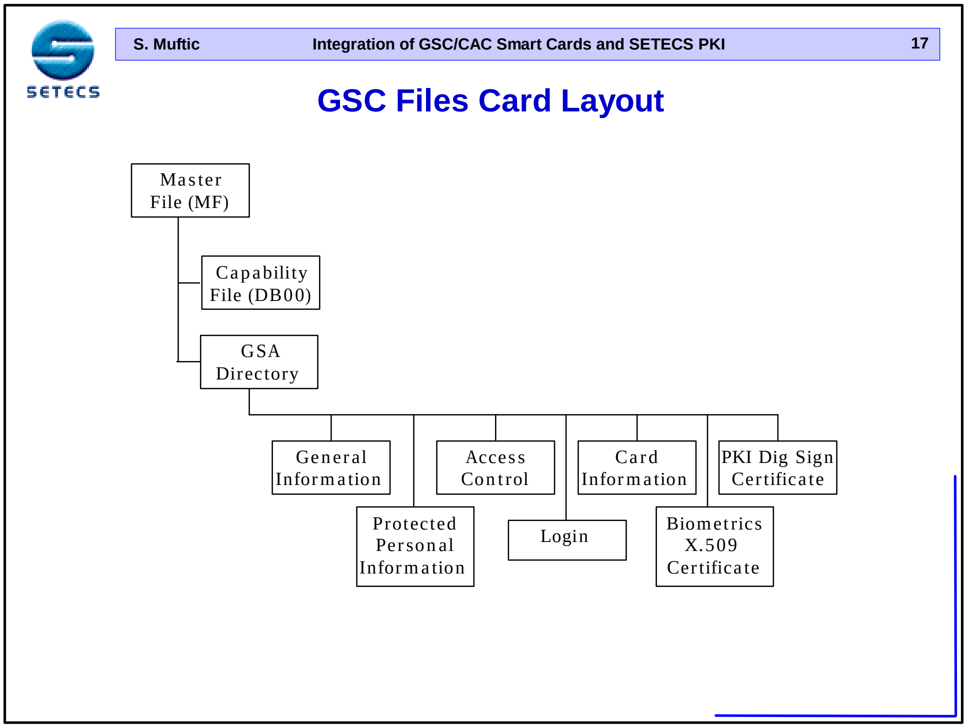
gscBsiGcDataCreate()
gscBsiGcDataDelete()
gscBsiGcReadTagList()
gscBsiGcReadValue()
gscBsiGcUpdateValue()

Utility Provider

gscBsiUtilAcquireContext()
gscBsiUtilCardConnect()
gscBsiUtilCardDisconnect()
gscBsiUtilGetACR()
gscBsiUtilGetBsiVersion()
gscBsiUtilGetCardProperties()
gscBsiUtilGetCardStatus()
gscBsiUtilGetExtendedErrorText()
gscBsiUtilGetReaderList()
gscBsiUtilPassthru()
gscBsiUtilReleaseContext()

Cryptographic Provider

gscBsiGetChallenge()
gscBsiSkiInternalAuthenticate()
gscBsiPkiSign()
gscBsiPkiGetCertificate()
gscBsiGetCryptoProperties()



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 17

GSC Files Card Layout

Master File (MF)

Capability File (DB00)

GSA Directory

General Information

Access Control

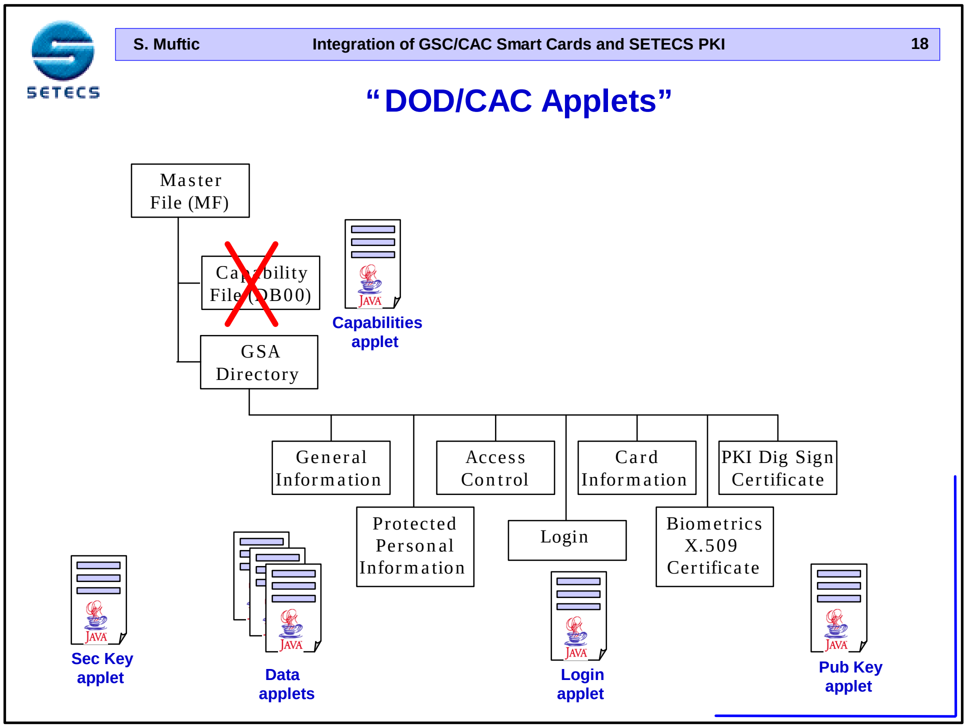
Card Information

PKI Dig Sign Certificate

Protected Personal Information

Login

Biometrics X.509 Certificate



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 18

"DOD/CAC Applets"

Master File (MF)

~~Capability File (DB00)~~

Capabilities applet

GSA Directory

General Information

Access Control

Card Information

PKI Dig Sign Certificate

Protected Personal Information

Login

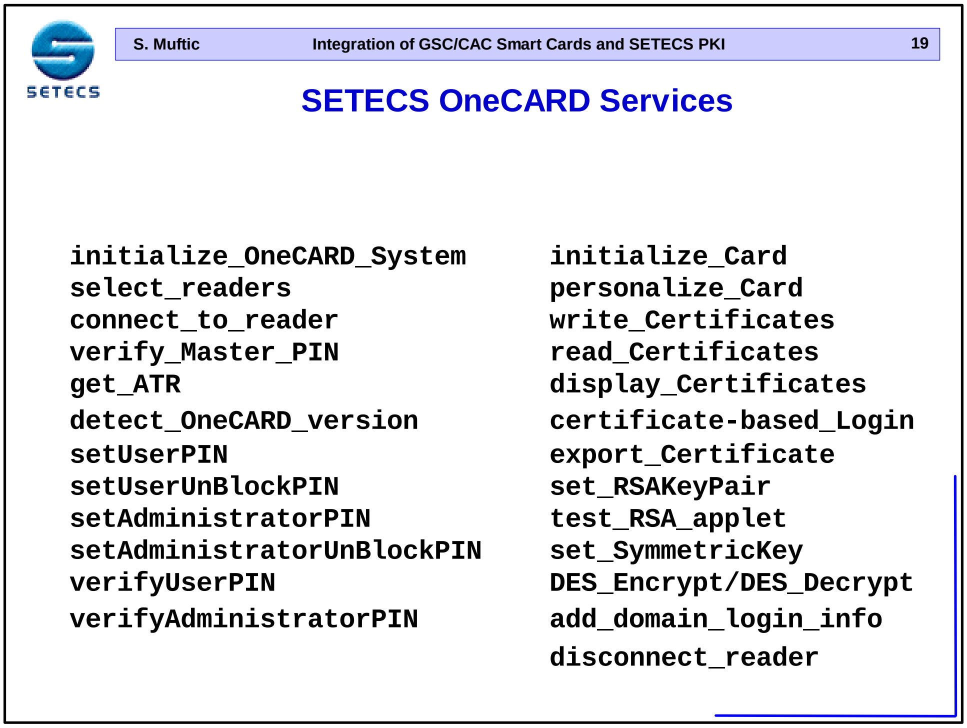
Biometrics X.509 Certificate

Sec Key applet

Data applets

Login applet

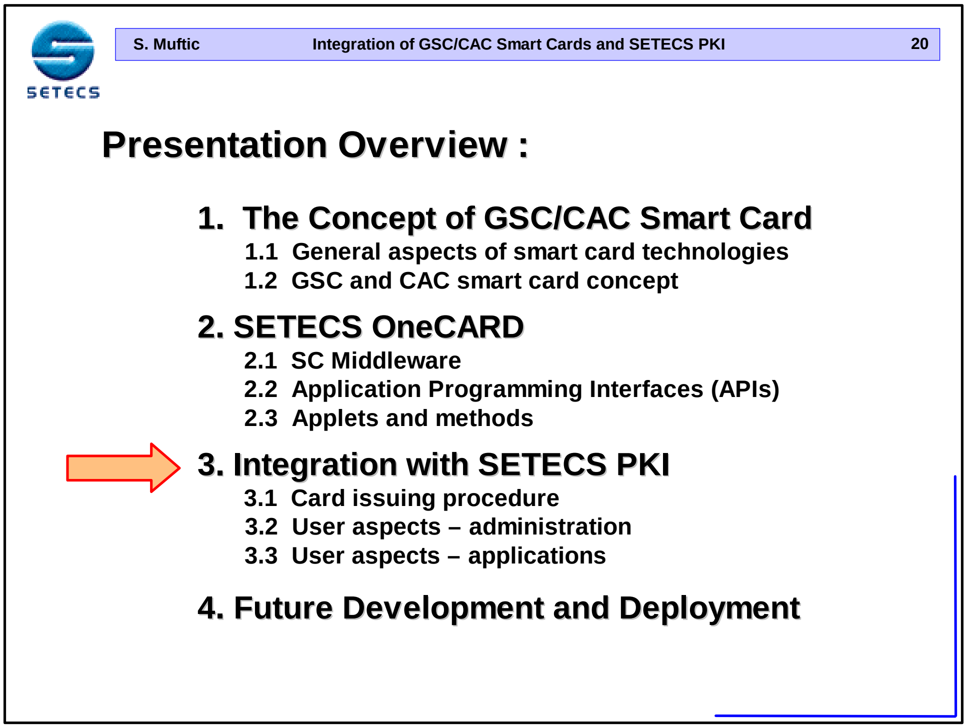
Pub Key applet



SETECS OneCARD Services

initialize_OneCARD_System
select_readers
connect_to_reader
verify_Master_PIN
get_ATR
detect_OneCARD_version
setUserPIN
setUserUnBlockPIN
setAdministratorPIN
setAdministratorUnBlockPIN
verifyUserPIN
verifyAdministratorPIN

initialize_Card
personalize_Card
write_Certificates
read_Certificates
display_Certificates
certificate-based_Login
export_Certificate
set_RSAKeyPair
test_RSA_applet
set_SymmetricKey
DES_Encrypt/DES_Decrypt
add_domain_login_info
disconnect_reader



Presentation Overview :

1. The Concept of GSC/CAC Smart Card
   1.1 General aspects of smart card technologies
   1.2 GSC and CAC smart card concept

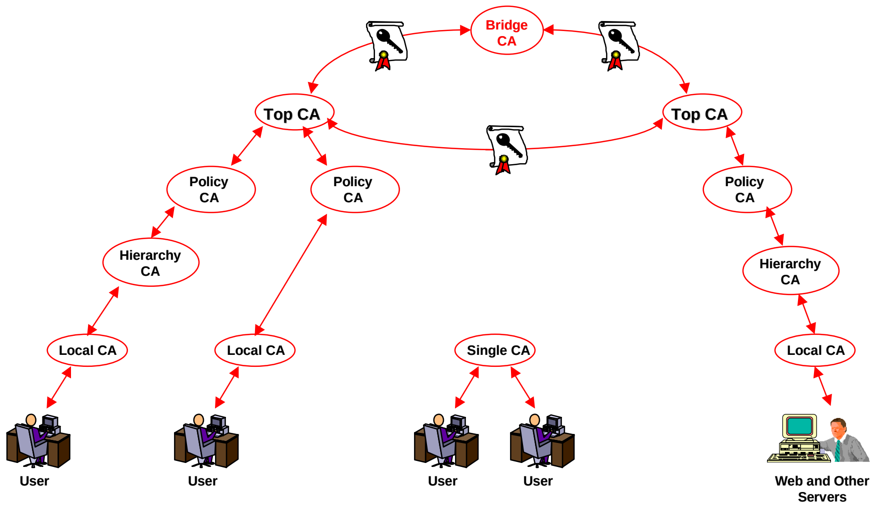
2. SETECS OneCARD
   2.1 SC Middleware
   2.2 Application Programming Interfaces (APIs)
   2.3 Applets and methods

3. Integration with SETECS PKI
   3.1 Card issuing procedure
   3.2 User aspects – administration
   3.3 User aspects – applications

4. Future Development and Deployment

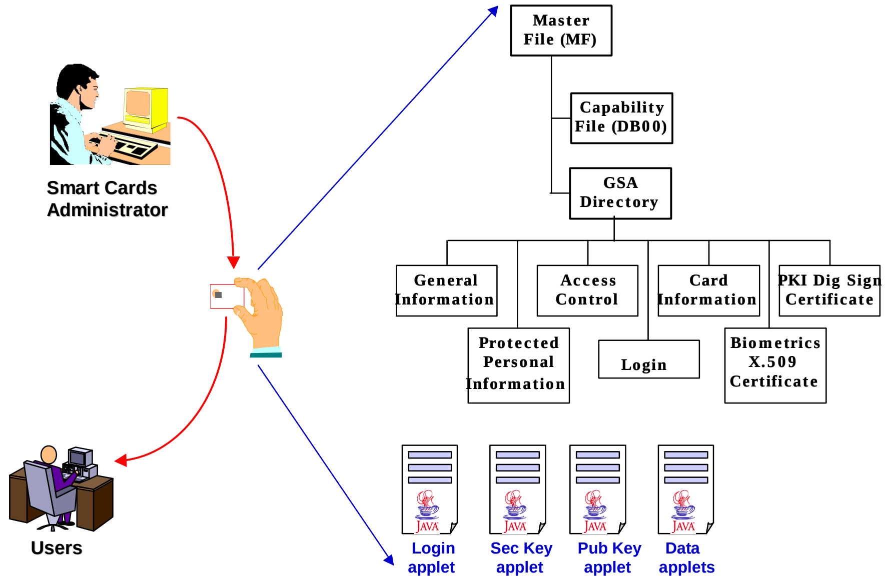
S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 21

SETECS One PKI – “Bridged” PKIs

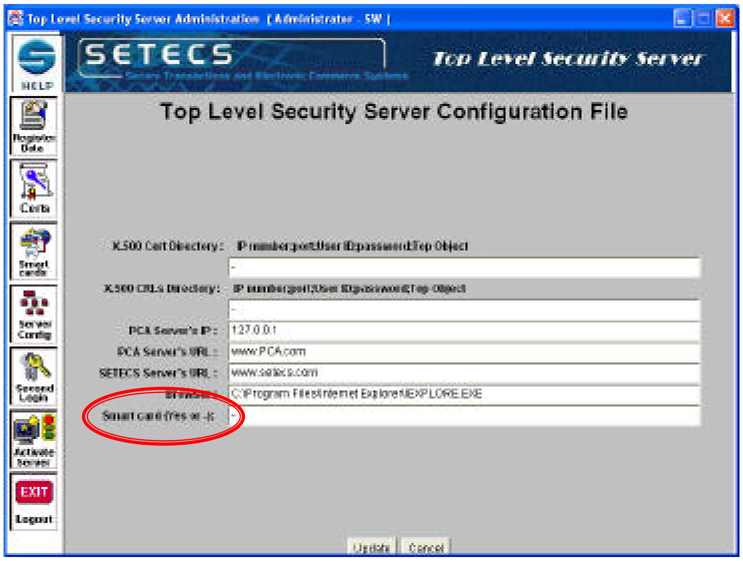


S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 22

Smart Cards Administration



Integration with CA Servers



Top Level Security Server Administration (Administrator - SW)
SETECS
Secure Transactions and Electronic Commerce Systems
Top Level Security Server
HELP
Register Data
Certs
Smart cards
Server Config
Second Login
Activate Server
EXIT
Logout
Update
Cancel

Top Level Security Server Configuration File

X.500 Cert Directory: IP number:port:User ID:password:Top Object
-

X.500 CRLs Directory: IP number:port:User ID:password:Top Object
-

PCA Server's IP: 127.0.0.1

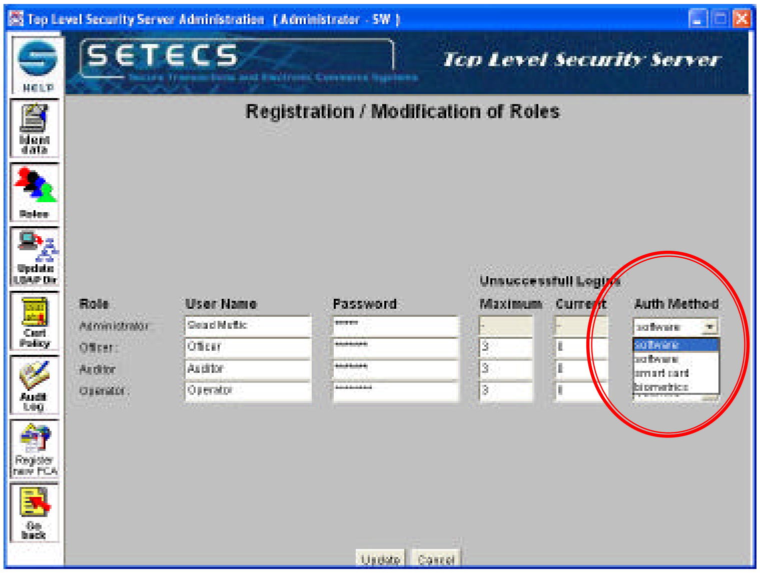
PCA Server's URL: www.PCA.com

SETECS Server's URL: www.setecs.com

Browser: C:\Program Files\Internet Explorer\IEXPLORE.EXE

Smart card (Yes or -): -

Multiple CA Administrative Roles

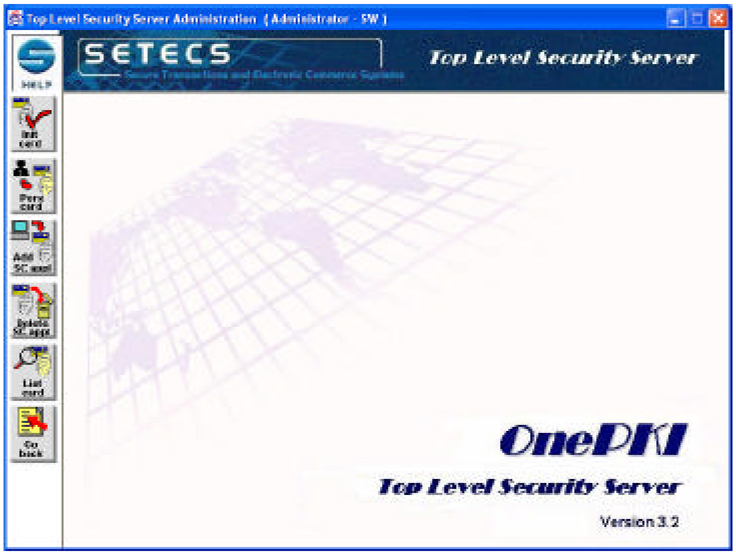


Top Level Security Server Administration (Administrator - SW)
SETECS
Secure Transactions and Electronic Commerce Systems
Top Level Security Server
HELP
Ident data
Roles
Update LDAP Dir
Cert Policy
Audit Log
Register new PCA
Go back
software
smart card
biometrics
Update
Cancel

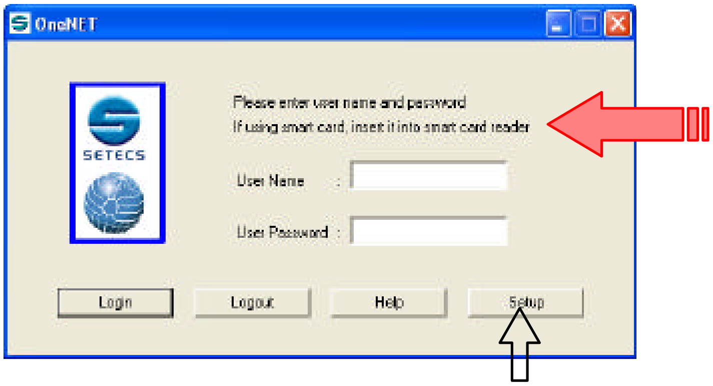
Registration / Modification of Roles

			Unsuccessfull Logins		
Role	User Name	Password	Maximum	Current	Auth Method
Administrator:	Sead Muftic	******	-	-	software
Officer:	Officer	********	3	0	
Auditor:	Auditor	********	3	0	
Operator:	Operator	*********	3	0	

Smart Cards Administration


Top Level Security Server Administration (Administrator - SW)
SETECS
Secure Transactions and Electronic Commerce Systems
Top Level Security Server
HELP
Init card
Pers card
Add SC appl
Delete SC appl
List card
Go back
OnePKI
Top Level Security Server
Version 3.2

Smart Cards – User Login



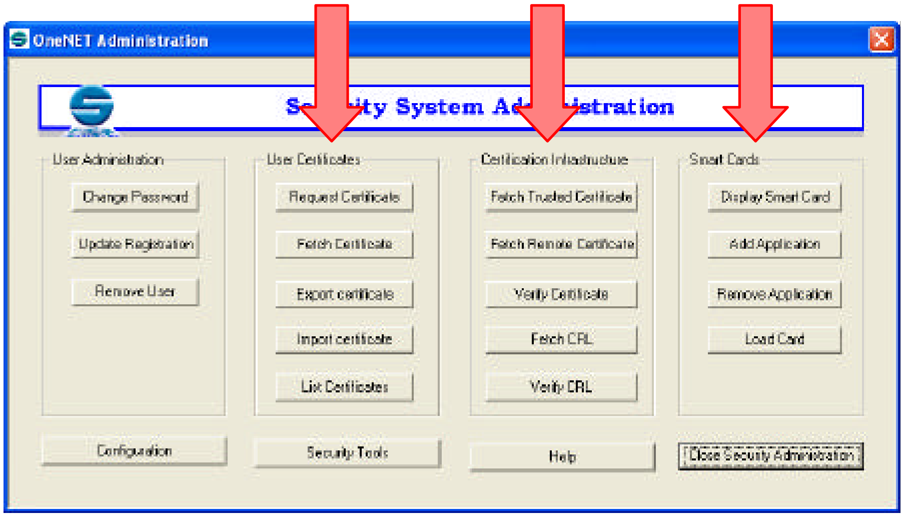
Please enter user name and password

If using smart card, insert it into smart card reader

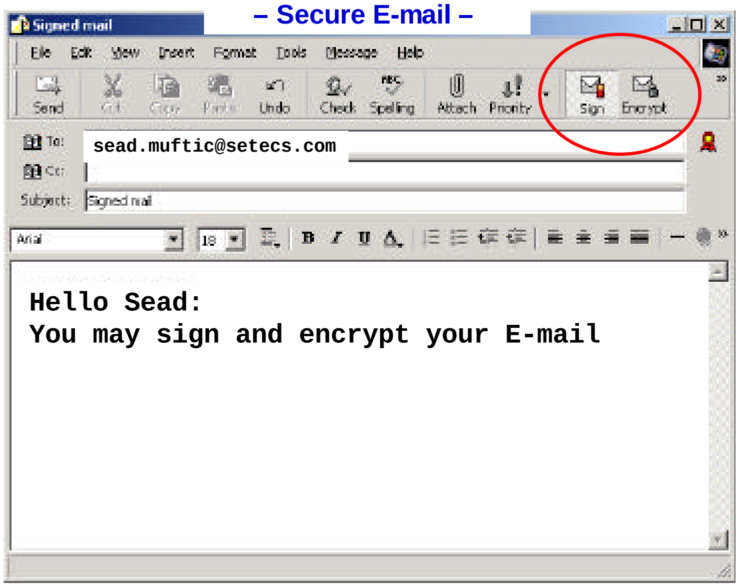
User Name :

User Password :

Smart Cards – User Administration



Secure Applications
– Secure E-mail –


Signed mail
File Edit View Insert Format Tools Message Help
Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt
Arial
10
B I U

To: sead.muftic@setecs.com

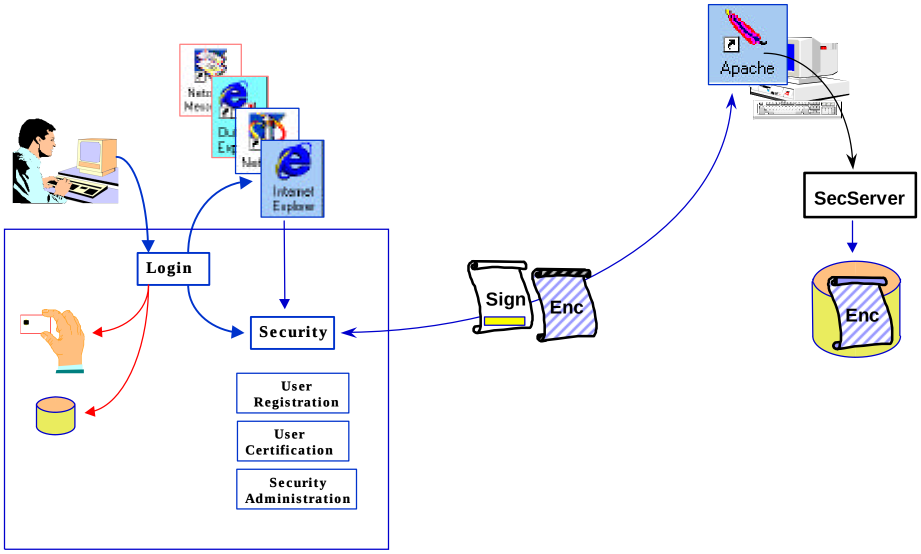
Cc:

Subject: Signed mail

Hello Sead:
You may sign and encrypt your E-mail

S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 29

Secure WWW (XML/HTML Documents)



S. Muftic Integration of GSC/CAC Smart Cards and SETECS PKI 30

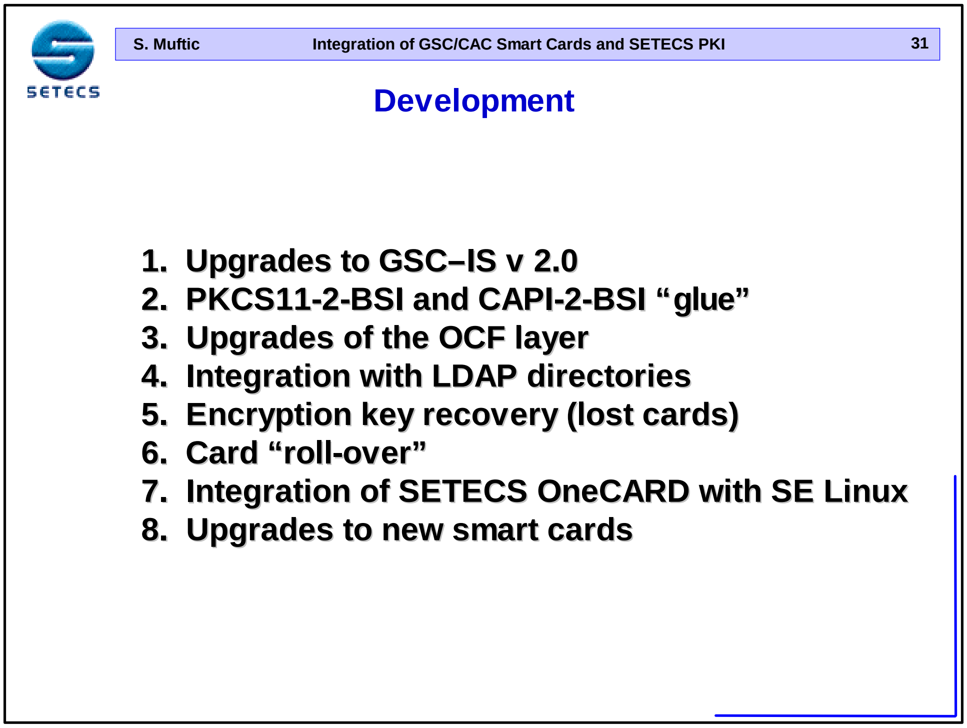
Presentation Overview :

1. The Concept of GSC/CAC Smart Card
   1.1 General aspects of smart card technologies
   1.2 GSC and CAC smart card concept

2. SETECS OneCARD
   2.1 SC Middleware
   2.2 Application Programming Interfaces (APIs)
   2.3 Applets and methods

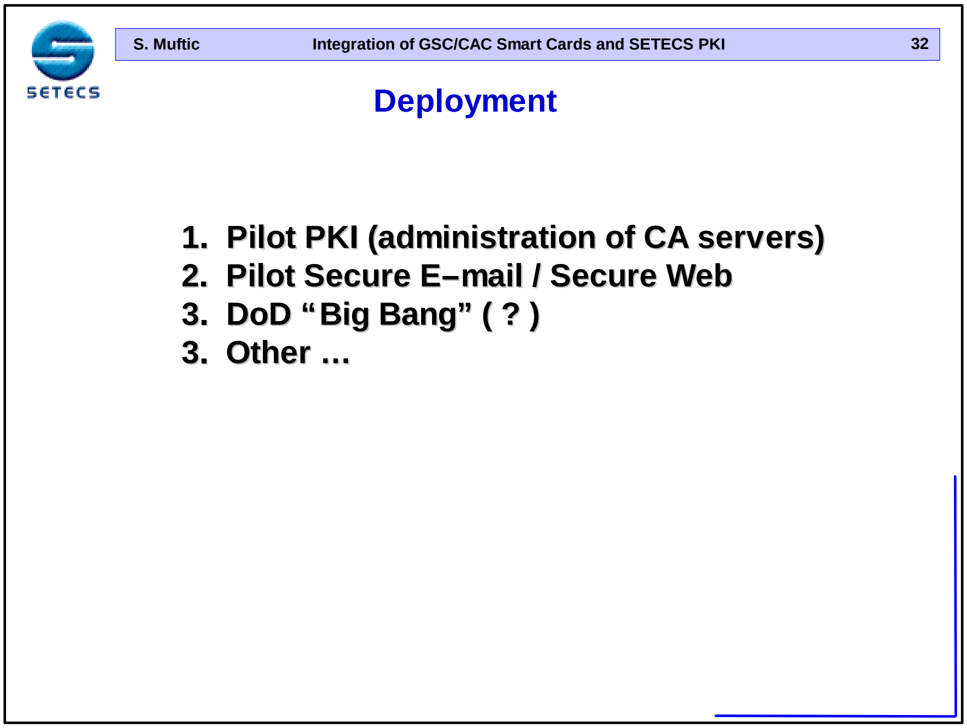
3. Integration with SETECS PKI
   3.1 Card issuing procedure
   3.2 User aspects – administration
   3.3 User aspects – applications

4. Future Development and Deployment



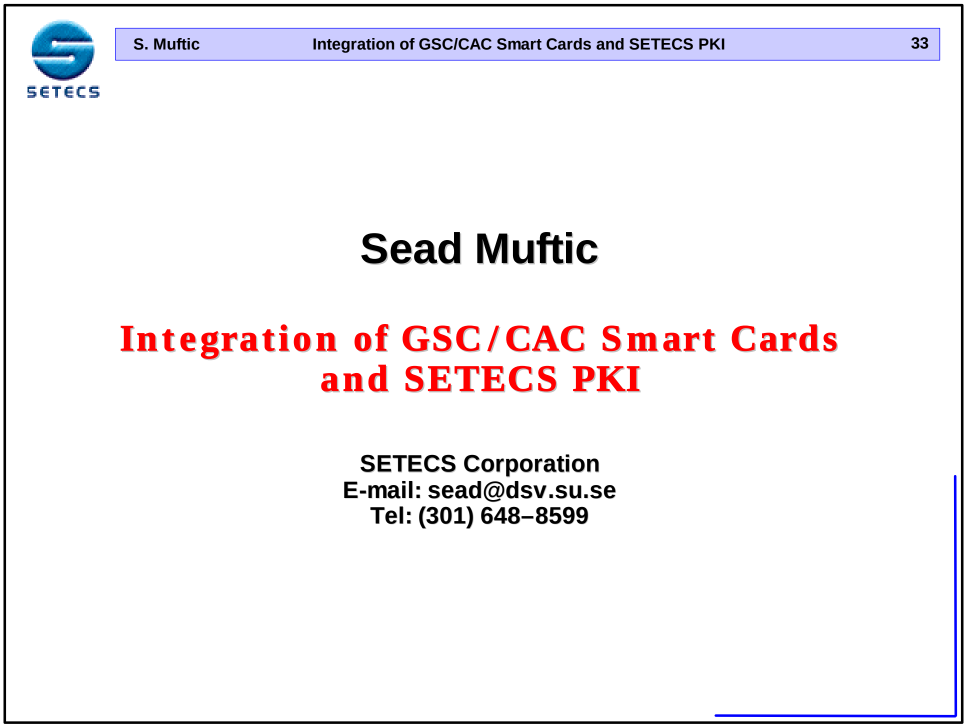
Development

1. Upgrades to GSC–IS v 2.0
2. PKCS11-2-BSI and CAPI-2-BSI “glue”
3. Upgrades of the OCF layer
4. Integration with LDAP directories
5. Encryption key recovery (lost cards)
6. Card “roll-over”
7. Integration of SETECS OneCARD with SE Linux
8. Upgrades to new smart cards



Deployment

1. Pilot PKI (administration of CA servers)
2. Pilot Secure E–mail / Secure Web
3. DoD “Big Bang” (?)
3. Other …



Sead Muftic

Integration of GSC/CAC Smart Cards and SETECS PKI

SETECS Corporation
E-mail: sead@dsv.su.se
Tel: (301) 648–8599