GT 50 改善

VISIONARY INNOVATORS

Cryptography

practice implementations

Sandro Fontana,
CEO GT50 sandro.fontana@gt50.org

in Bruce Schneier we trust ⟶ Applied Cryptography 2nd edition 1996

Who we are

GT50 is a Visionary Innovators Company
We are focused in turning technology into real worth applications

GT50 people has got more than 30 years experience in digital security and data protection

We are engaged in combining different existing and robust technologies - like Sym/Asym Cryptography 2D Timbro Digitale and QR Code - to enhance Security and application of Digital Certification Solutions

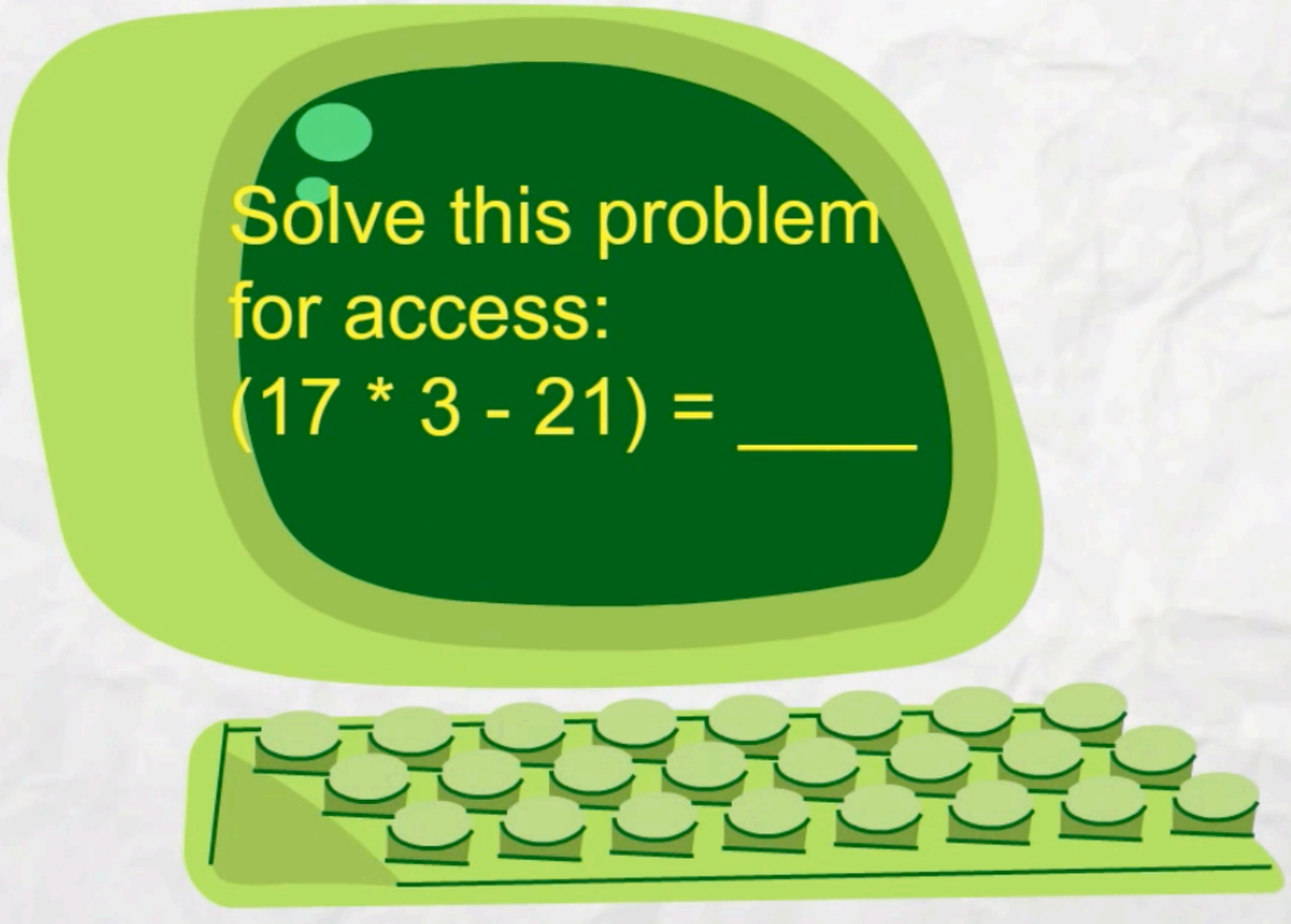
Our Mission is turning technology into real Value Added Applications, keeping the best standards in term of security of the process managed

We give Technical Service and Support to more than 100 Customers - Public and Private Market - provided with "Timbro Digitale" Solutions: 2D-Plus and Lambda

We also provide our customers with Consulting Services

there are two kind of cryptography in this world:

cryptography that will stop your kid sister from reading your files, ...



there are two kind of cryptography in this world:

... and cryptography that will stop major governments from reading your files.

http://bit.ly/GT50-Videos

Cryptographic Suite:
ETSI (EU)
NIST (USA)

other sources:
ISO
RFC

to avoide case like
Kuznyechik block cipher
&
Streebog hash function
http://bit.ly/2E2XL9S

GT 50 改善
VISIONARY INNOVATORS

what we do

Timbro Digitale

RSA2048
SHA256
XML/XSL

CAdES

LAMBDA SERVICE

RSA2048
SHA256
AES256

PAdES

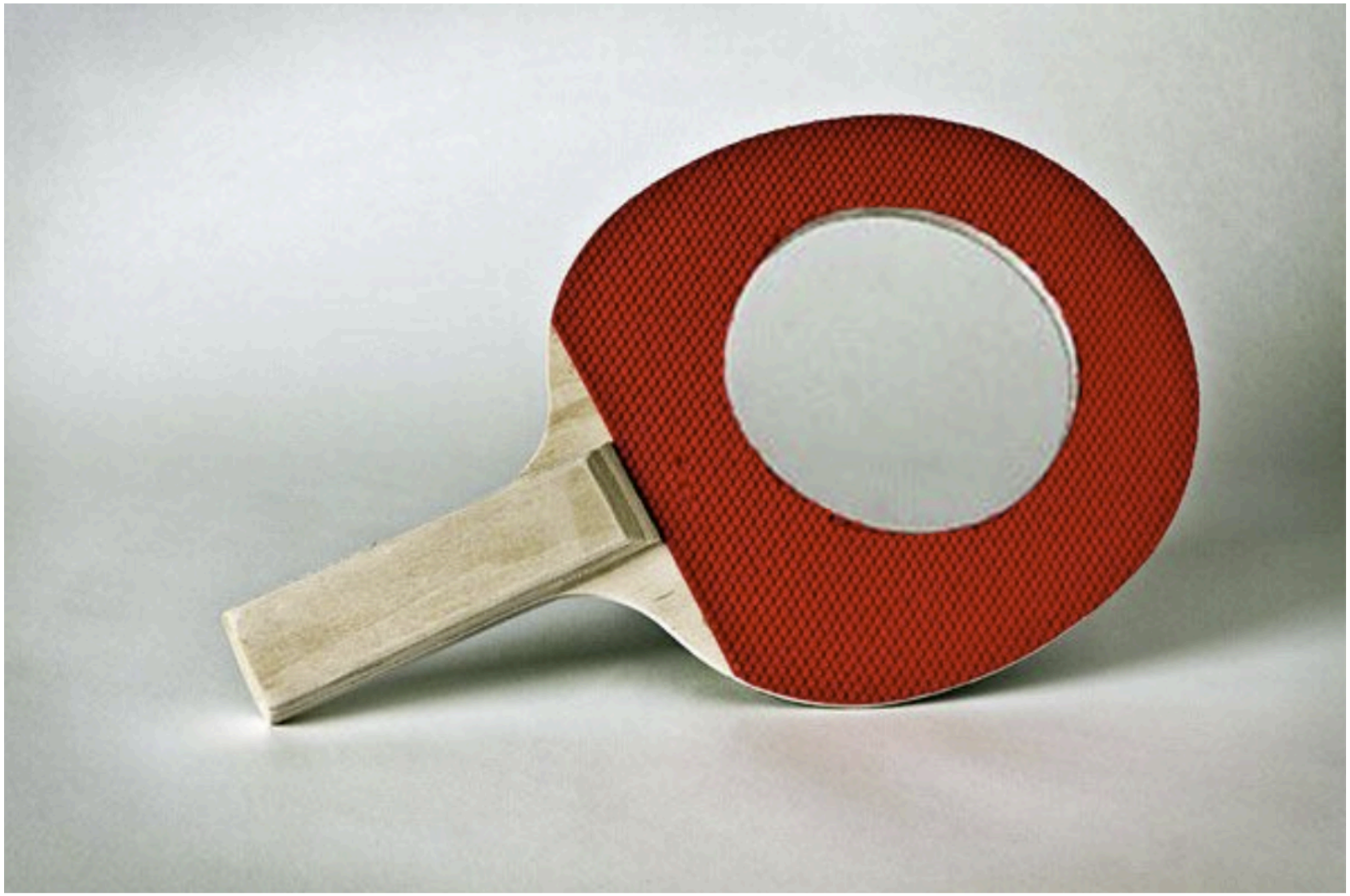
Q-ID

RSA1024/2048
SHA256
BCrypt
AES256
OATH rfc4226 / rfc6238
OCRA rfc6287
QRCode

PhotoShield

RC4
SHA256

Timbro Digitale



how about the value of
the printing of a digitally signed document?

Paper e-Sign®: digital signature on paper

Sandro Fontana
Secure Edge S.r.l.
s.fontana@computer.org

ACM, AICA, ICSA, IEEE, ISOC, USENIX

Abstract

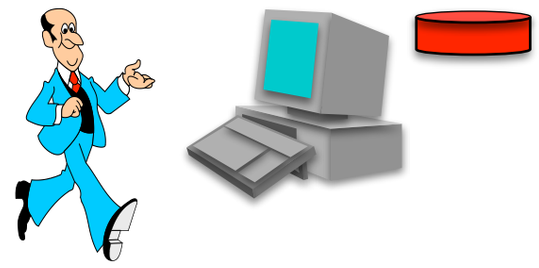
La tecnologia di firma digitale è accettata ogni giorno di più come la soluzione che permette lo scambio di documenti rispettando le caratteristiche d'integrità, non ripudiabilità ed autenticità. La catena del valore del documento elettronico è così rinforzata, consentendo nuove possibilità nel B-to-c e nel B-to-b. Il mondo reale però necessita ancora della carta e qui nascono i problemi, perché il processo di stampa interrompe la catena del valore della firma digitale.
L'articolo che segue, introduce una metodologia che permette agli utenti di mantenere inalterata questa catena del valore ed in alcune situazioni di renderla ancora più robusta.

The digital signature technology is being accepted more and more as the solution that enables the exchange of digital documents fulfilling the requirements of integrity, non-repudiation, and authenticity. The value chain of electronic documents is thus reinforced, allowing new possibilities for B-to-c and B-to-b. In everyday life though, we still need paper documents but the printing process breaks the value chain of digitally signed documents.
The following article introduces a methodology that allows the user to maintain unaltered the value chain of digital signatures. Moreover, in some cases, it reinforces the process

what it is

It is a large capacity two-dimensional graphic code, which acts as a data container/file [digitally signed]

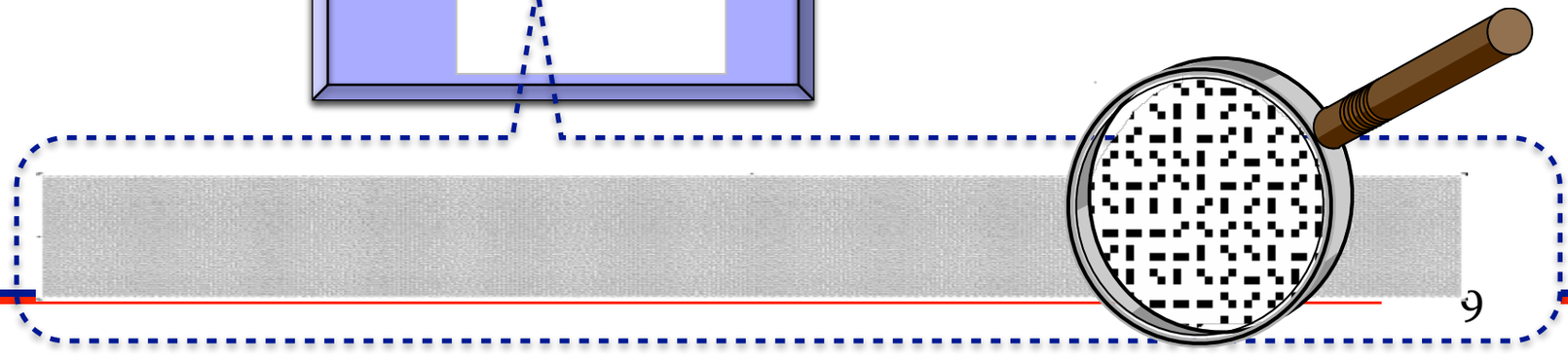
data:
RTF, ASCII, XML ...
digitally signed:
PKCS#7, CAdES



Bob

Alice

dati:
RTF, ASCII, XML ...
digitally signed:
PKCS#7, CAdES



contents

.xml.p7m (CAdES)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<?xml-stylesheet type="text/xsl" href="nome_file.xsl?SHA256= B8D150 … 61DB5766E”?>
<TD:Global xmlns:TD="http://www.timbrodigitale.org/TD_tags">
        <TD:XSL_Def>
            <TD:orig>http://www.comunedioizo.com/xsl/</TD:orig>
        </TD:XSL_Def>
      <TD:C2D-Plus>
            <TD:AppCode>201</TD:AppCode>
      </TD:C2D-Plus>
   </TD:Global>

<root_node>
...
</root_node>
```


COMUNE DI RAVENNA

SERVIZI DEMOGRAFICI

CERTIFICATO DI RESIDENZA

IL SINDACO

In conformita' agli atti d'ufficio
CERTIFICA CHE:

PURITANI ANNA
Nata il 05/06/1955 a Milano
Atto n. 1767 p.1 a.A
Abitante in Via Stradone n. 177/C
RAVENNA

E' proven. da Milano il 31/10/1979 pr. 1191
Motivo richiesta: miei motivi personali

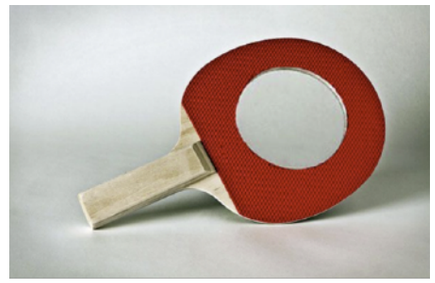
Ravenna , 31-03-2009

IL SINDACO

we can validate the external file .xsl
by means of its SHA256 value

what it is

Lambda Service allows you to generate digitally signed PDF (PAdES) documents, customizing the signature area, in which a special secure QRCode (Lambda Seal) is inserted.



Dichiarazione Sostitutiva di certificato di iscrizione al Registro Imprese della Camera di Commercio (Art.46 e 47 D.P.R. del 28 Dicembre 2000):

Il sottoscritto **Sandro Fontana**, Nato a Roma prov. Roma il 13/02/1955, Residente in Roma via Salvatore D'Amelio n.15 00167,
Consapevole delle **sanzioni penali**, nel caso di dichiarazioni non veritiere, di formazione o uso di atti falsi, richiamate dall'art.76 del D.p.r. 445 del 28/12/2000,

DICHIARA

Di essere il Legale Rappresentante dell'Impresa **GT50 Srl.**
Sede Legale **Via Filippo Corridoni 19 00195 Roma.**
Codice Fiscale **10707081005** P.IVA **10707081005**
Iscritta al Reg. Imp. di **Roma** dalla data **04/12/2009** costituita con atto del **23/11/2009**

Dati relativi agli Amministratori muniti del potere di rappresentanza (cariche, dati anagrafici e codice fiscale): NULLA

Oggetto sociale in sintesi: **IDEAZIONE E REALIZZAZIONE DI SISTEMI DI SICUREZZA INFORMATICA**
Sedi Secondarie e unità locali
Sede Operativa: viale degli Ammiragli n. 67 00136 Roma

DICHIARA INOLTRE

che l'impresa non si trova in stato di fallimento, di liquidazione coatta, di amministrazione controllata o di concordato preventivo e che nei confronti della stessa non sono in corso procedimenti per la dichiarazione di tali stati;

Luogo e Data
Roma 13/02/2018

IL DICHIARANTE

VISIONARY INNOVATORS
Firmato da: Fontana Sandro
CF: TINIT-FNTSDR55B13H501Y
Titolo: Amministratore Unico
Azienda: GT50
Firmato il: 2018/11/20 17.07

La copia su carta è conforme all'originale firmato in formato PAdES. Leggere il QrCode per accedere al documento originale

Lambda Seal

signature area

Moreover: A) a crypted copy (AES256) of PAdES file is stored in cloud:
the only instance of the key is contained in Lambda Seal
B) if requested, an "entry" is generated into FACTOM blockchain
as notarization

GT 50 改善
VISIONARY INNOVATORS

contents

signature area

Lambda Seal

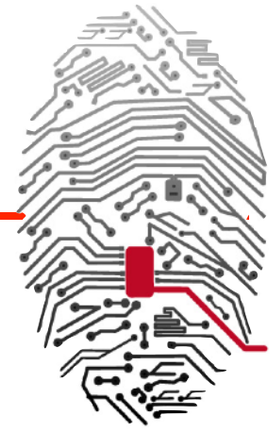
contains metadata needed to retrieve the (encrypted) PAdES file from the cloud and the unique key to decrypt it

The contents could be sealed using
RSA 2048
(not standard format seal)

Universal QReader™ a free App for smartphones and tablets, downloadable from PlayStore(Android) and AppStore(IOS)

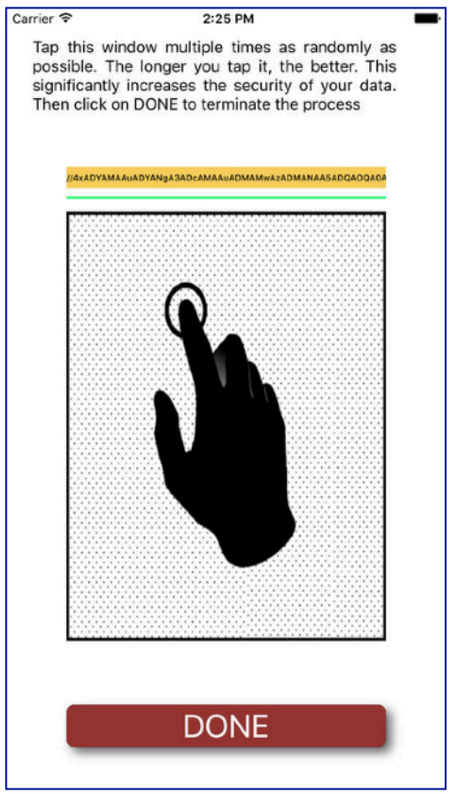
GT 50 改善
VISIONARY INNOVATORS

Q-ID: privacy keeper



Functions:

- Password Wallet
- Virtual One Time Password Tokens [vToken] event/time based
- Virtual Smart Cards [vSCard] for AdES for signing (RSA1024/2048)
- Secure message exchange (AES256)
- Protection of personal data
- Synchronization between devices



Everything is protected by a Master Passphrase (user level) and a key derivation function BCrypt based, with a high computational cost.

Randomness is increased by data derived from user behaviour.

LibQID Controller

2FA

The platform supports both OATH-compatible hardware tokens and virtual tokens
It is Implemented in the form of a stand-alone C library for Linux-like environment

Google
Facebook
Snapchat
Evernote
Dropbox
Synology
Wordpress
...

OTP Seeds are generated within certified hardware devices; they are sealed (RSA2048) and crypted (AES256), than sent to the Authentication System Administrator. (customer side)

When seeds are acquired from LibQID Controller, they are further transformed within and under the control saldo cedolino Aprile 2019 of the Client's System

in this way, no useful information remain in GT50 hands

GT 50 改善
VISIONARY INNOVATORS

Q-ID: another use case

As it is physically independent of the hardware used, you can use Q-ID OTP in many other controlled access applications.
e.g. a virtual token allows quick access control via integrated control turnstiles or remote control.

As it is based on a One-Time-Password, the virtual token cannot be used more than once, making physical access control very secure.

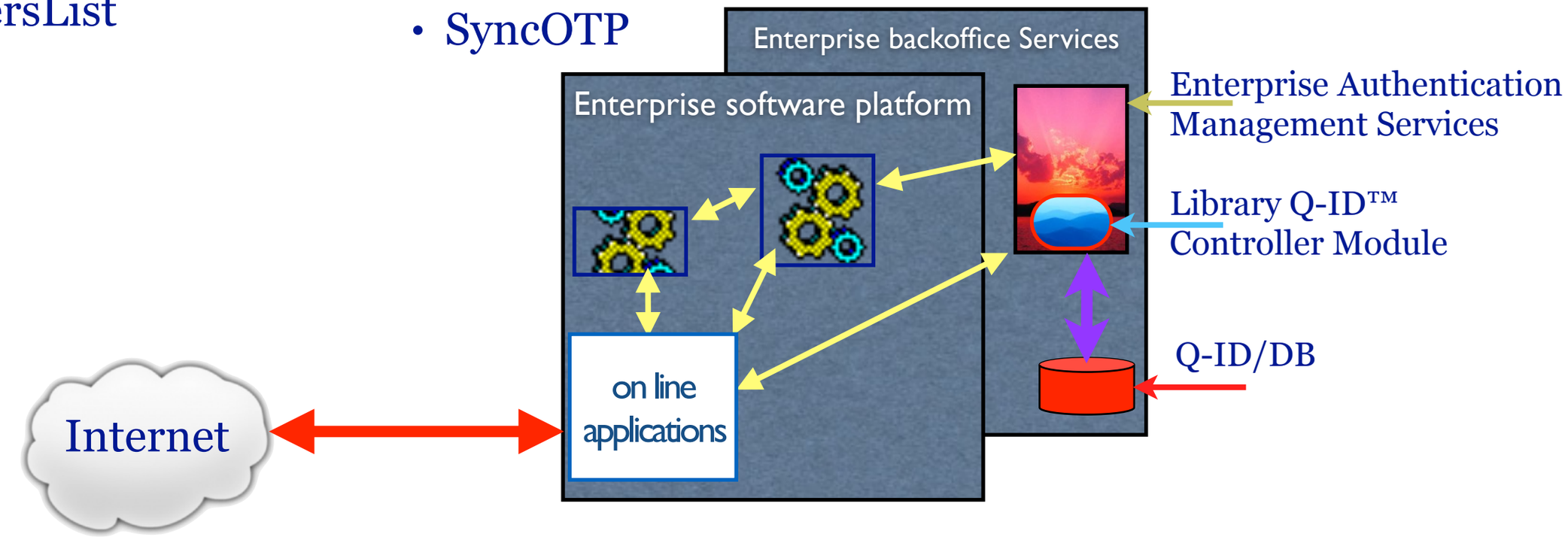
LibQID Controller: API

Admin Functions:

- ShowLibVersion
- DestroyAll
- DBCheck
- DBUpdate
- LibInit
- AddLicense
- AddLicenseUpdate
- SetupOTPParams
- SetEDesc
- Stats
- GetUsersList

Operating functions :

- GetErrorMessage
- AddUser
- ResetUser
- DelUser
- UserStatus
- GenSQA
- GenSQAU
- GenSQE
- VerOTP
- VerOTPE
- SyncOTP

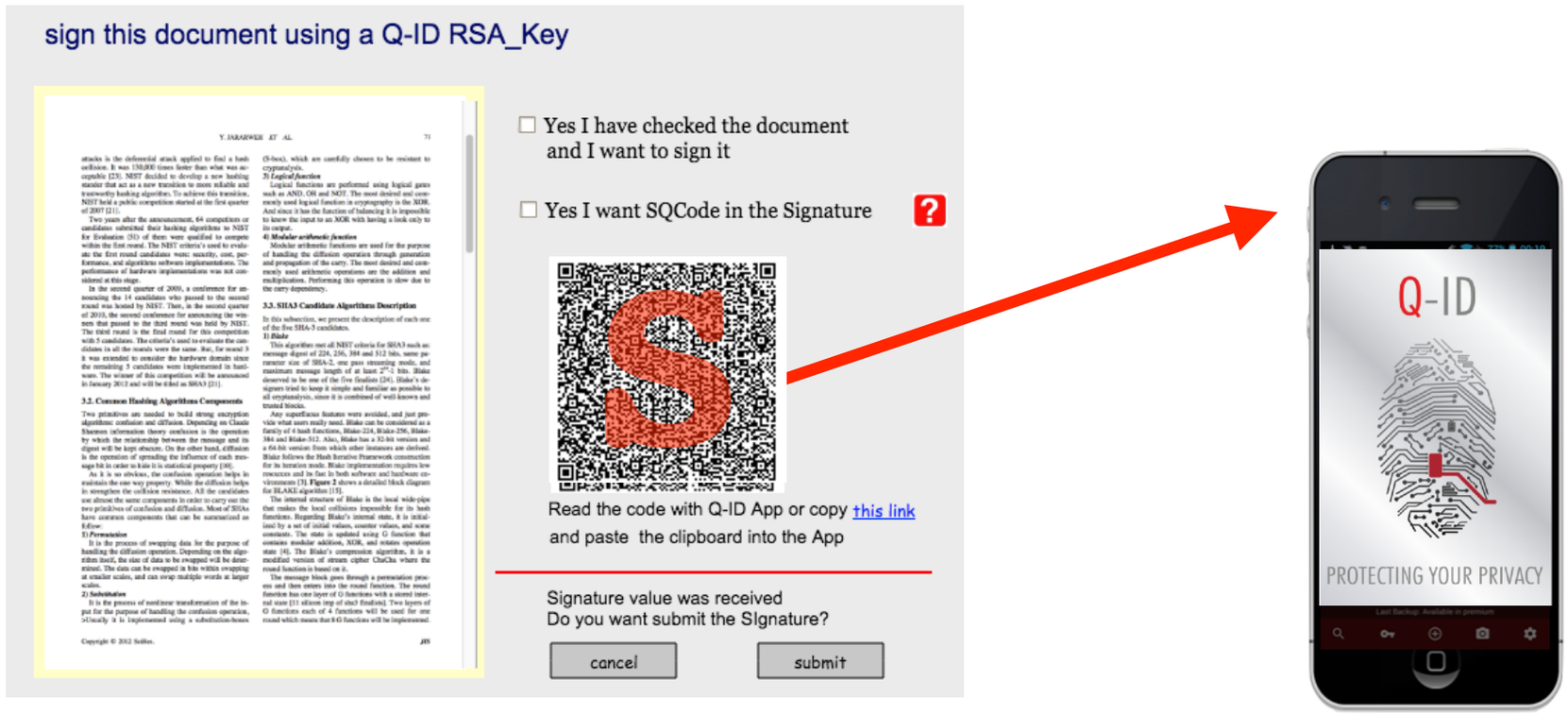


LibQID Controller

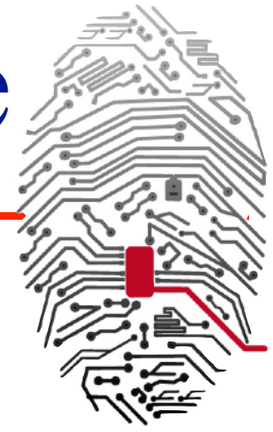
Electronic Advanced Signature (RSA)

The great versatility and processing capability of smartphones allows the Q-ID™ App to be used also in the field of Advanced Electronic Signature

The Q-ID™ App has the ability to read SQCodes and evaluate their semantics. In this case, an AdES (RSA) request is submitted; the final signature format is PAdES (or CAdES).



Secure message exchange



PGP/GPG Like

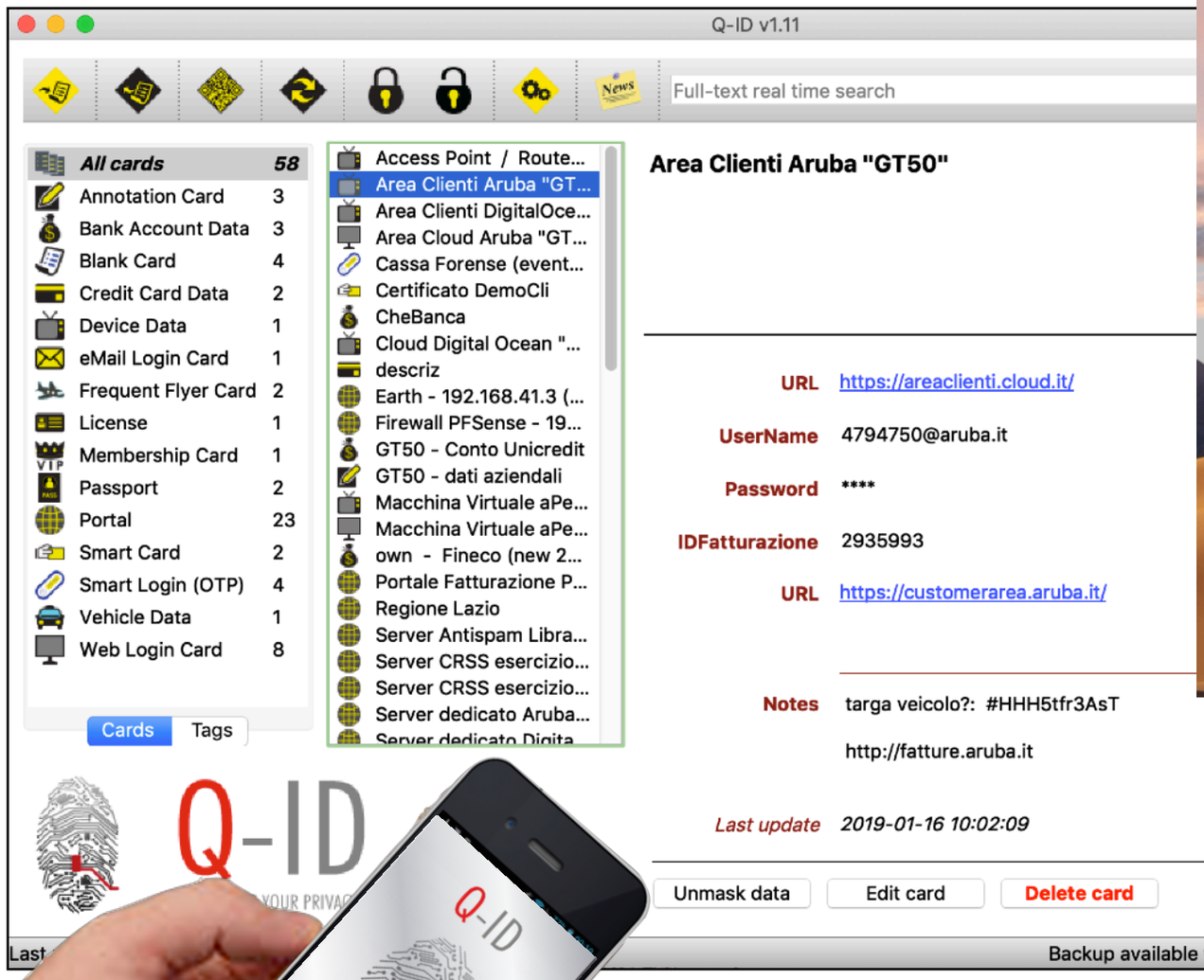
The platform supports the exchange of encrypted data (AES256), with a PGP/GPG style

-----BEGIN Q-ID MESSAGE-----
Version: 1.6.1 Mac - www.q-id.org

svxbkVESaugP2pQKV/nmR4w7dMSNC9gPnRPKXrNAlvHU9OM6Lo7DiuloN4Yj6v6xHtBxYZscrB2x
NlBXLKGvBTJcE3oL5w24bDpxL0AVGw3cYXhJlat6lmRLo+Qnq0Rp33tftQlOEzcWS/4O4nZJzh3m
OHIXL/jD6sP4/uzxpdcTJszBra+F8SUDvnHC4mE3jrk/tdWeWH00X4u5UhtKVL5Felm3Mlu7DPUC
TGXJmdzngI6/JZLyVYhKgiUFxEySZFYKK7DnphLQZ27ApfDBGihtS/oZDAX0XOt3ycbUr8PmpZ6B
VWTI8YVwD0fI2Y6WchDxb0q6/7mDXQVdUAlGREegXbS189lgL0j1MIc5crmSBl5hM0BeByOKDV4h
yAldcsnVfg5hWbNhtLSfqn+CGwXVH3oo8vZAM7LSLGZjK6OSeAq5J3s+T6krHSYRcPay6kD2wUGb
QB0EuCeuLJePsxbj1IAsSQtliqQajiXyZL9BDs2Yg0JC9cGy7XikePS4u4mIk88bykKkirJlOHQB
sy0bnj0JLWuxXwaIzMz2J8wAMyR4UA6zV1CLxeuJv7IUaea88Cx41B//pXdBO1TC8YfiESKO0uEd
FxP6RyYJkTgBemQGkZtaG4/nTmN7wc/dxzSMusQh/llBAVuGPRYiCru8dYs37qUrrvHhsjTPaZ6y
Pw7y//5ACzvOvmsb33WLL2MWl0J7/nwMla7FaBM0yQZ9pljTmG0Mp2ohuNAEFvnPVBkNuF8v/Y4v
dSFYzryVXnRuw4y9AaYqHvOPQgjgn7jTc7cFgyClHmXNJlfs6X7GL88rw1Z8mHUwGbJPY9Jr6TKx
krj3LiQNRexXDOLdr+juTAKRQ7OlXctONOCXu2b3cWuuvscAhPSWqzx9LmwKmYKnor9ULR3opweC
E0TMN1Pbgnc3aueBwxEZWncXq9S18TU4RUe0zCP9/rCoNFsxXWv8+La75vlN34ccllqrGDEi5cVu
H/XTBsc3meaCkgM1AyzGlsG8cVtHi5cGH+9LbilUHhSGAp83yVd1tjDUeGa4T2YmagjzPqdXm8jv
VYlislKxcrsVfhKefM6ysqzxvtCJ1hDez1PvVf3pW5+gCSuSvvalUNUZ5XCMClDwtRM1p7cccale
YwTOGeOUjgLWcoUD49IQun/DCbRCRopnFjlleWvtlorc12yT7v5oDwYtd3TkVieWG9Y7BEXrteoN
CUvVppcFxUk3vcDTt/CK9Bf/lF+FSXjUnCodw+uP46vfWQ1HH94VC5quaeE4Fvxkom6Yea8h+w26
N/DNoh2hR6DjAZ0E4XikzK5WGobfVGtaw1r90r8uoSo7a7eOlKXopEGSKbDUrGiGOveovTd5o3ri
6ZodewF8L8U3nIEOz2n8Ajk6sj+dhAeTITlbcZ2xmE61ohIW6Aim6aJEFk4Vl5jRAUQaE9FHlF0Q
QY1QHZ+F9u/oqmG6FibvVcwZ2Ssl2FcFewkb/mQtQSUpqa2PJg===hLTz
-----END Q-ID MESSAGE-----

GT 50 改善
VISIONARY INNOVATORS

Mobile & Desktop App



Q-ID™ is a free App:
for smartphones and tablets, downloadable from PlayStore(Android) and AppStore(IOS);
Windows and OSX versions downloadable from https://www.q-id.net

PhotoShield

All of us using our smartphone or our tablet to take pictures of ourself, of our friends and of a lot of thing that happen around us.

The exchange of personal images,
has become a common usage between young people and not only.

Such data can become more vulnerable once uploaded online and we have to remember that "The Network Never Forgets".

Often the involuntary disclosure of these images,
can cause severe damage to the reputation.

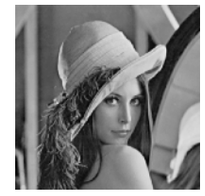
GT 50 改善
VISIONARY INNOVATORS

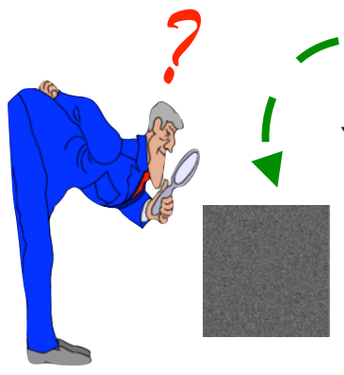
PhotoShield

This is the reason because we develop PhotoShield

Using this application,
you will be able to exchange your personal pictures with your friends,
without fear that other people can see them.

Your private images will stay private,
because protected by a scrambling process.





You will be able to archive the scrambled pictures
in your smartphone or in the cloud,
with the confidence that
no other will be able to access to the original pictures in intelligible form.

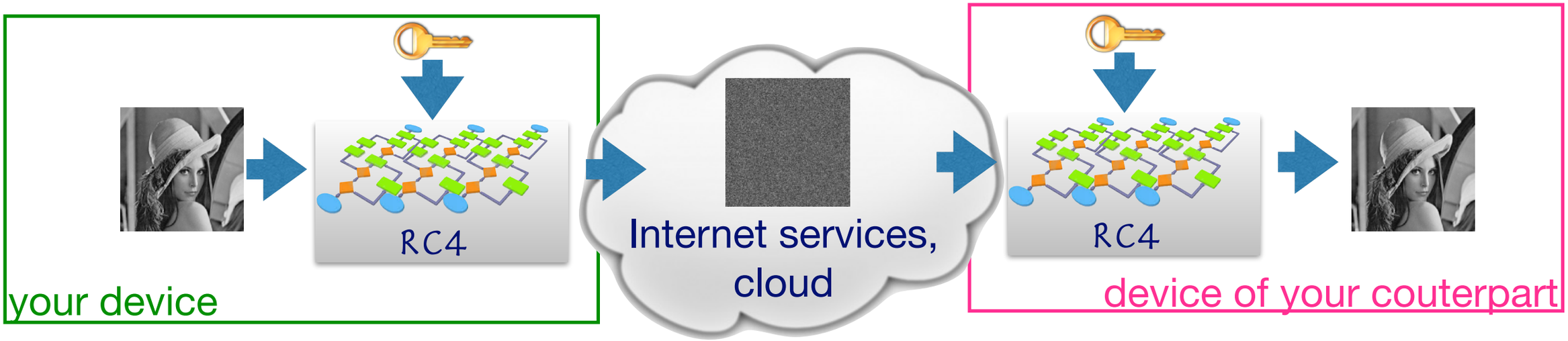
PhotoShield

How we decide the reorganization of the blocks?

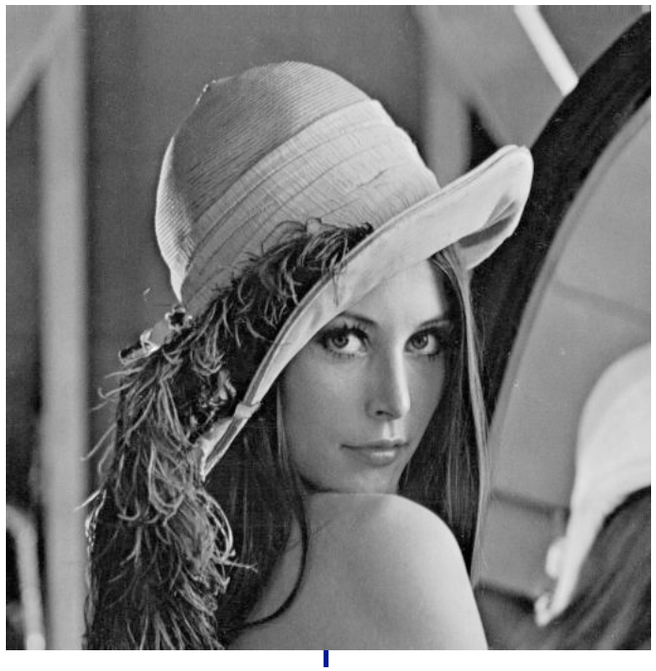
We use a stream cipher generated by an RC4 implementation
as pseudo random index generator:
that define the new coordinates for each pixels-block of the picture.

The password -that you have chosen to protect the picture-
generate a different sequence of coordinates;
these scramble the original picture in a unique way.

Using the same password,
only your counterpart will be able to rebuild the original image.

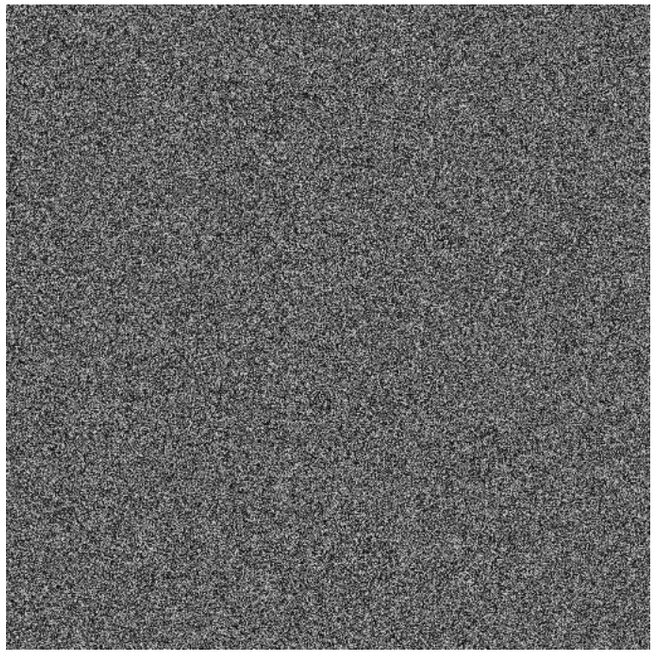


more the granularity, less the meaning

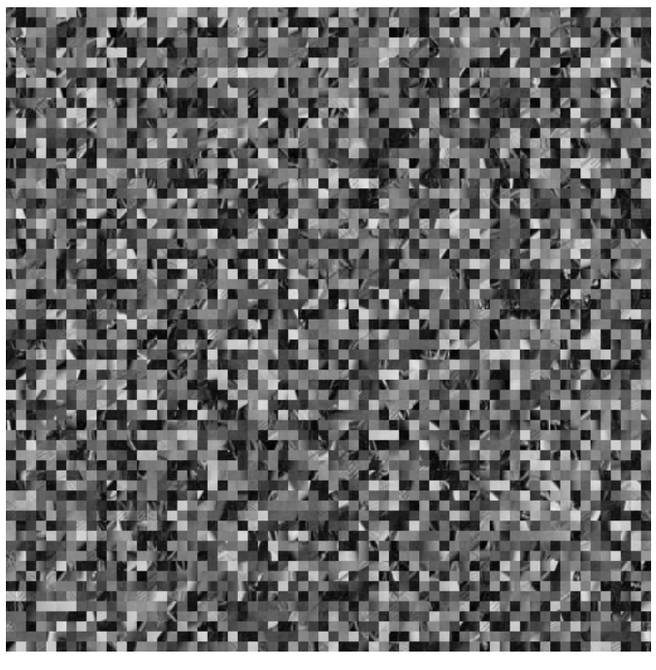


256pixels*256pixels block
reorganize 4 blocks

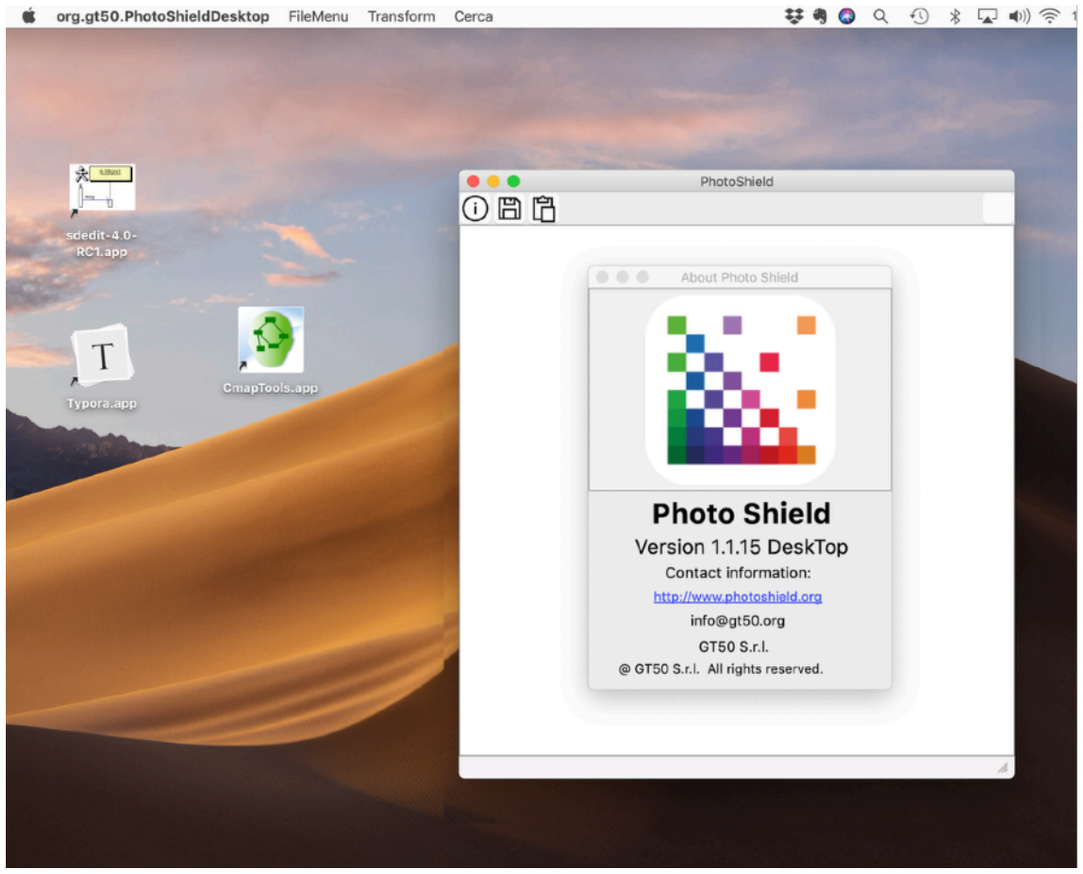
1pixel*1pixel block
reorganize every single pixel



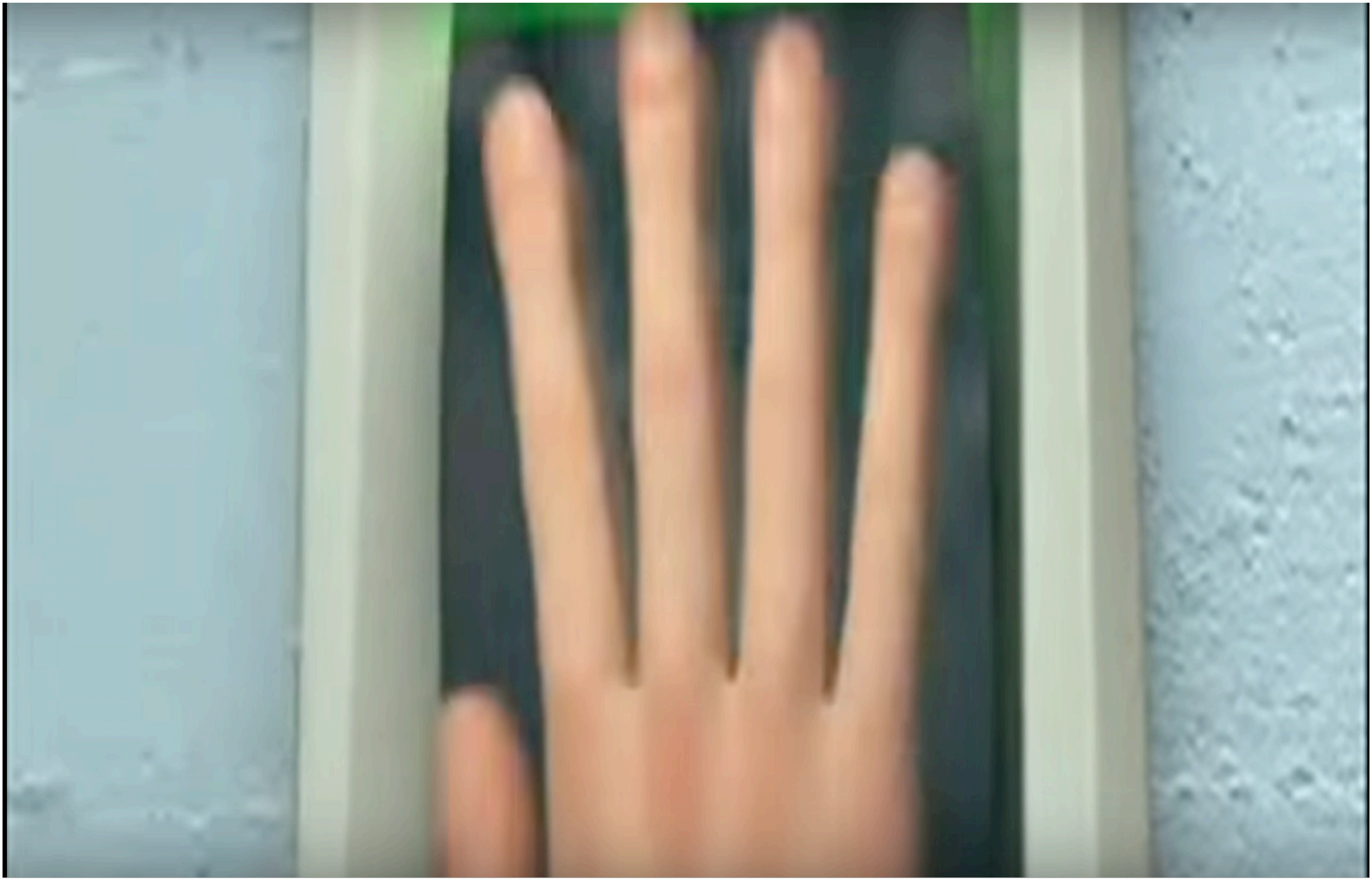
8pixels*8pixels block
reorganize 4.096 blocks



Mobile & Desktop App



PhotoShield™ is a free App:
for smartphones and tablets, downloadable from PlayStore(Android) [IOS: soon];
Windows and OSX versions downloadable from https://www.photoshield.org



Thank you for your attention

Sandro Fontana, sandro.fontana@gt50.org
CISSP, ISO27001 L.A., CISM, CISA
skype/twitter: sinetqnlap
http://sandrofontana.com