The Security Aspects of e-APP

Assoc. Prof. Dr. Ahmet KOLTUKSUZ

<ahmet.koltuksuz@yasar.edu.tr>

Dept. of Computer Engineering

College of Engineering of Yaşar University

The *Apostille*

Definition:

«An **authentication** certificate issued by an authority designated by the State where the public document was executed. This certificate is called an *Apostille.*»

«How to join an implement the Hague Apostille Convention: A Brief Guide»

Components of an e-apostille:

#1 e-apostille issuing Competent Authorities

#2 e-Register

Types of e-Registers

Functionality	Category	Information displayed
Basic	Category 1	"Yes" / "No"
Additional (incl. *visual checks* of produced docs)	Category 2.1	"Yes" / "No" + basic description of underlying doc
	Category 2.2	"Yes" / "No" + image of Apostille or the underlying doc
	Category 2.3	"Yes" / "No" + image of the underlying doc + image of Apostille
Advanced (allowing for *digital verification* of produced docs)	Category 3.1	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille
	Category 3.2	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille + verification of integrity of underlying doc
	Category 3.3	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille + image of underlying doc

Definition of a Signature

A signature is a person's name written by him(her)self as a proof of authorship of the contents of a document.

Peculiarities of the Signature

The signature should be

- authentic,
- unforgeable,
- not reusable,
- unalterable,
- unrepudiable.

Attributes of an E-Signature

e-signature bears exactly the same attributes with that of an ordinary signature.

Thus, one must maintain them always by cryptographic security functions.

The document

From a fraudulent point of view, any e-document in electronic transaction so long as not protected with a digital signature can be

-disclosed to illegitimate persons **(problem of secrecy),**

-may be tampered with **(problem of integrity),**

-forged – reused & repudiated **(problems of authenticity).**

Security components

Attributes of a provable secure digital transaction

1. Secrecy
2. Integrity: Digital Signature
3. Authenticity

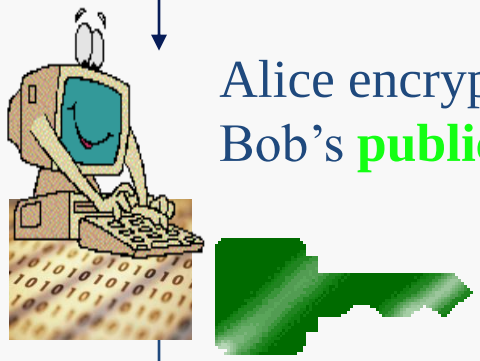
} ASYMMETRICAL CRYPTOSYSTEMS

These attributes should be maintained always!!!

Sender: Citizen Alice

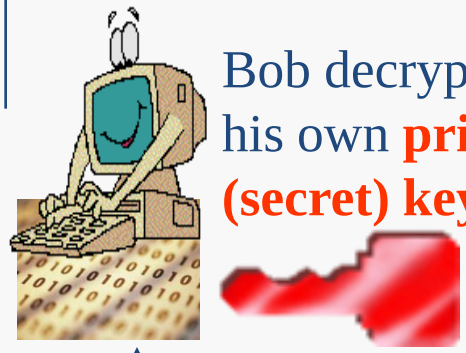
Receiver: Citizen BOB

plaintext

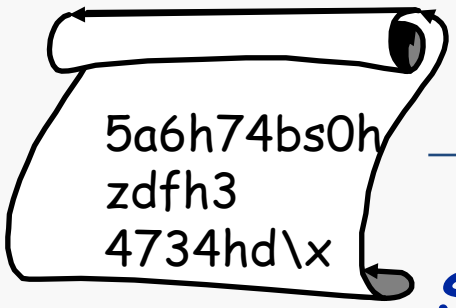


Alice encrypts with
Bob's **public key**

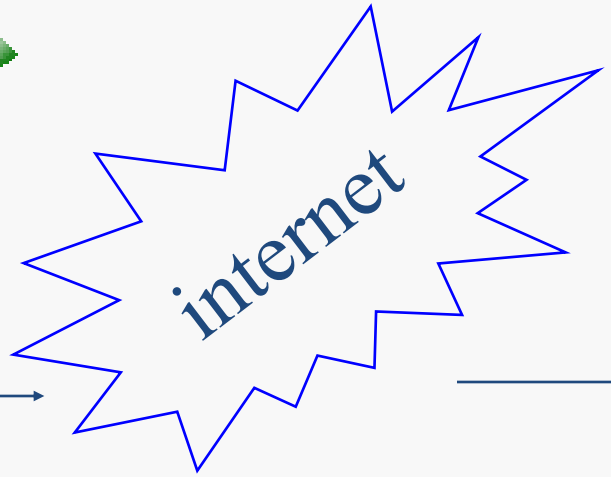
plaintext

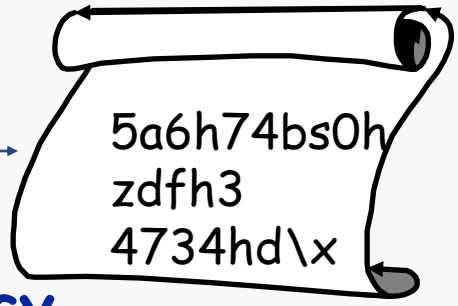


Bob decrypts with
his own **private
(secret) key**



ciphertext



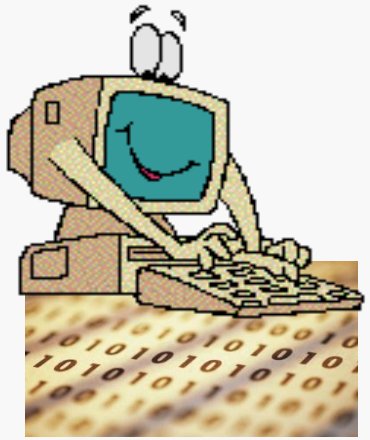


ciphertext

Scenario #1 The secrecy

Digital signature

plaintext



Apply hash function
Secure Hash Algorithm (SHA256)

Hash value

we09854jkl
)/(&hj37894

256 bits

Alice encrypts the hash value with her private (secret) key

\+

Hash value

we09854jkl
)/(&hj37894

=

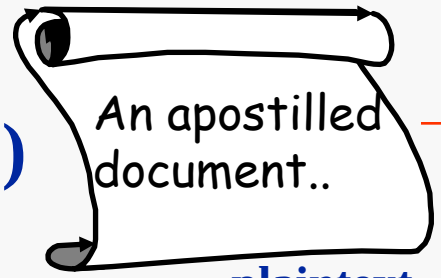
DIGITAL SIGNATURE

of Alice

Scenario #2 The integrity: Digital Signature

ALICE

1)

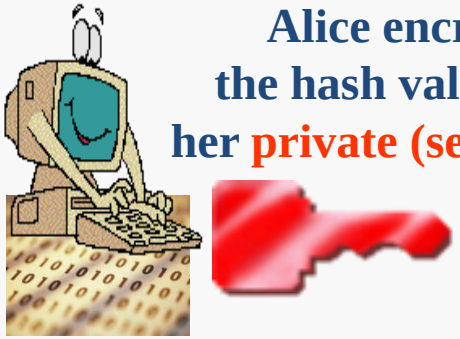


plaintext

→

Alice

+



Alice encrypts the hash value with her private (secret) key.

=

of Alice

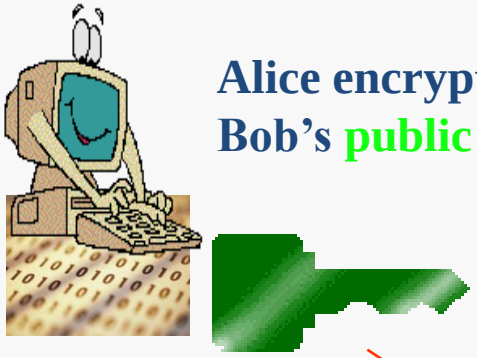
2)

plaintext

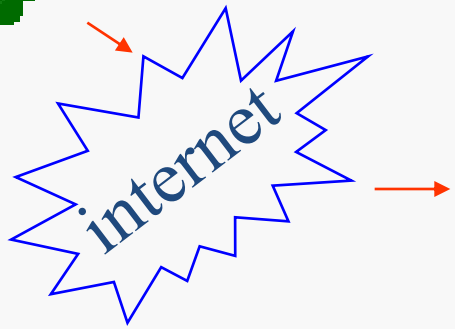
+

of Alice

→

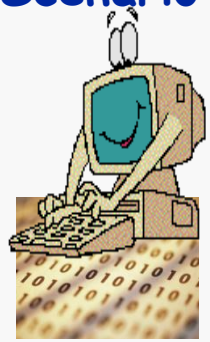


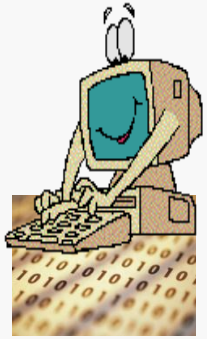
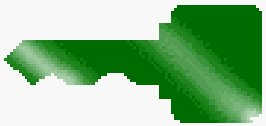
Alice encrypts with Bob's public key



Scenario #2 The integrity: Digital Signature

BOB

1)  Bob decrypts with his private(secret) key  = DIGITAL SIGNATURE of Alice + an apostilled document.. plaintext

2)  Bob decrypts with Alice's public key  + DIGITAL SIGNATURE of Alice = Hash we09854jkl)/(&hj37894 Alice

3)  Hash function + An apostilled document.. plaintext = Hash we09854jkl)/(&hj37894 Bob

4) Hash we09854jkl)/(&hj37894 Bob ? = Hash we09854jkl)/(&hj37894 Alice

YES: done!

NO: cancel the transaction

Scenario #3 Authenticity

- Using asymmetrical encryption in a superimposed fashion for the purpose of ID control.
- Means that the sender encrypts with his/her secret key first, followed by the encryption with the receiver's public key.

Scenario #3 The authentication

ALICE

1)

plaintext

Alice

+

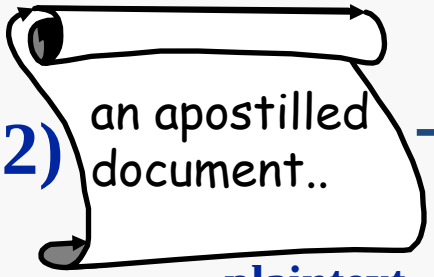
Alice encrypts
the hash value with
her private (secret) key.

=

DIGITAL SIGNATURE

of Alice

2)



plaintext

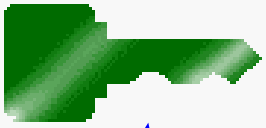
+

DIGITAL SIGNATURE

of Alice

Alice encrypts
all with her
private (secret) key.

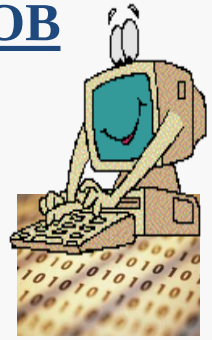
Alice encrypts
With Bob's
public key



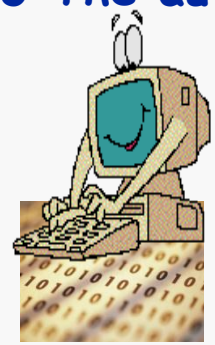
Scenario #3 The authentication

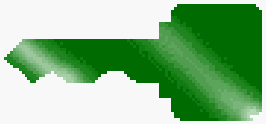
BOB

1) Bob decrypts all with his private(secret) key



Bob decrypts all with Alice's public key



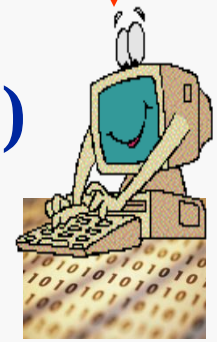


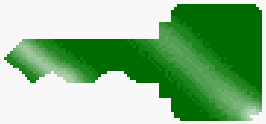
YES; continue.

NO

Cancel it! it's not AUTHENTIC!!!

2) Bob decrypts with Alice's public key





+ DIGITAL SIGNATURE of Alice = Hash we09854jkl)/(&hj37894 Alice

3) Hash function

+ Apostil.. plaintext = Hash we09854jkl)/(&hj37894 Bob

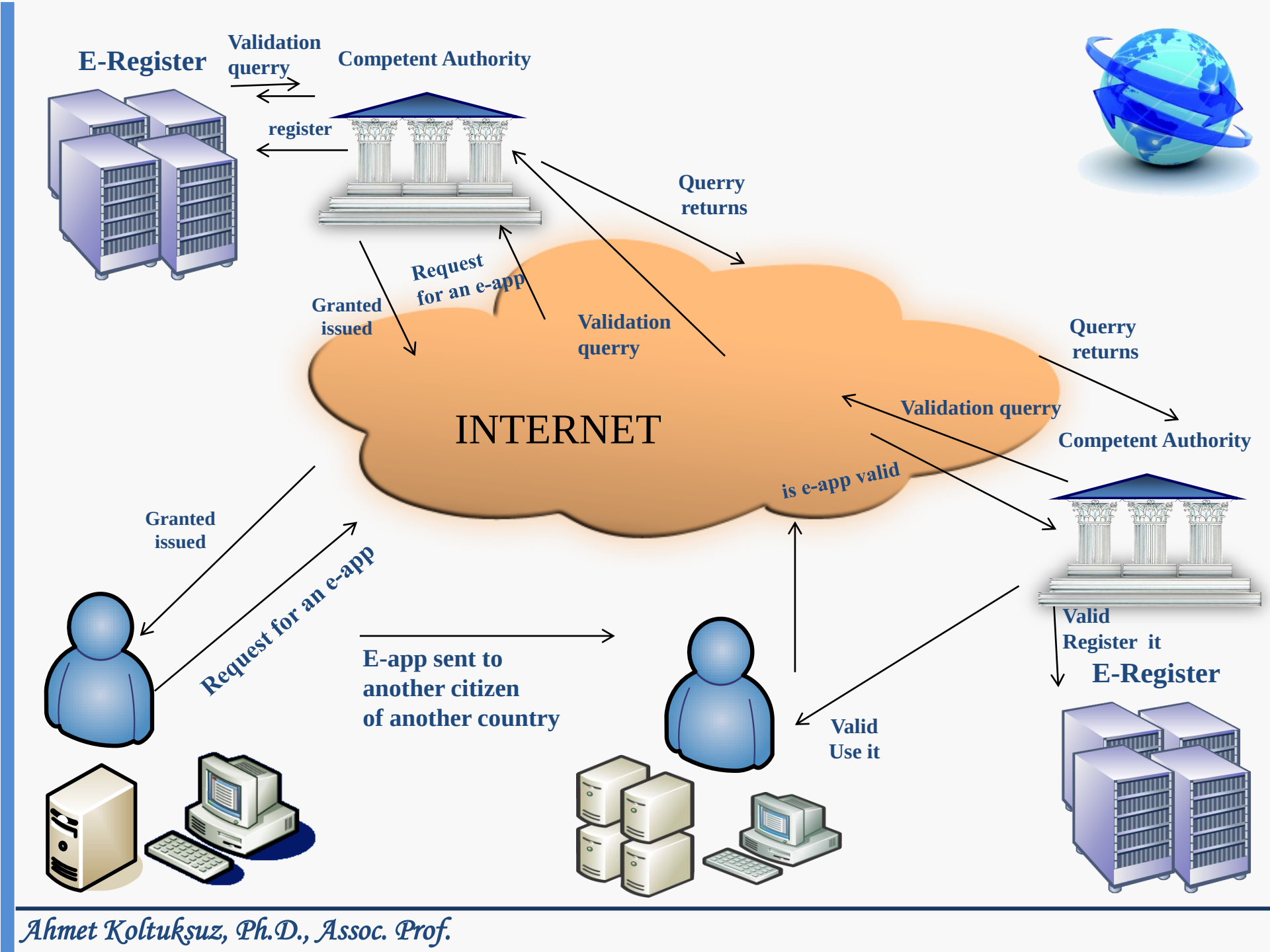
4) Hash we09854jkl)/(&hj37894 Bob ? = Hash we09854jkl)/(&hj37894 Alice

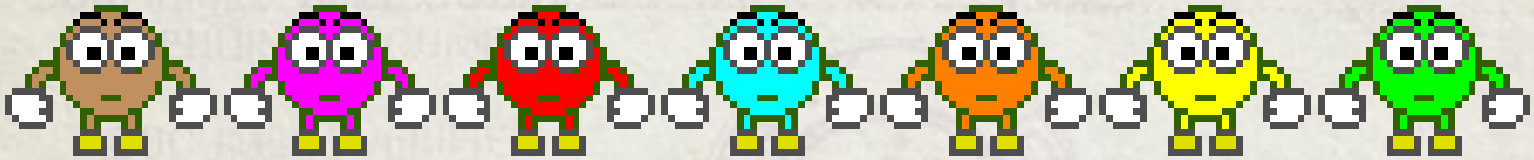
YES: Done.

NO: Cancel the transaction!!!

Types of e-Registers

Functionality	Category	Information displayed
Basic	Category 1	"Yes" / "No"
Additional (incl. *visual checks* of produced docs)	Category 2.1	"Yes" / "No" + basic description of underlying doc
	Category 2.2	"Yes" / "No" + image of Apostille or the underlying doc
	Category 2.3	"Yes" / "No" + image of the underlying doc + image of Apostille
Advanced (allowing for *digital verification* of produced docs)	Category 3.1	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille
	Category 3.2	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille + verification of integrity of underlying doc
	Category 3.3	"Yes" / "No" + image of Apostille + verification of digital signature on Apostille + image of underlying doc


E-Register
Validation querry
Competent Authority
register
Querry returns
Request for an e-app
Granted issued
Validation querry
INTERNET
Querry returns
Validation querry
Competent Authority
is e-app valid
Granted issued
Request for an e-app
E-app sent to another citizen of another country
Valid Register it
E-Register
Valid Use it



Thank you so much for your time & attention.

Ahmet KOLTUKSUZ

<ahmet.koltuksuz@yasar.edu.tr>