الشركة الليبية للبريد ،الاتصالات وتقنية المعلومات القابضة
Libya Post Telecommunication & IT Holding Company
LPTIC

TAQNYA

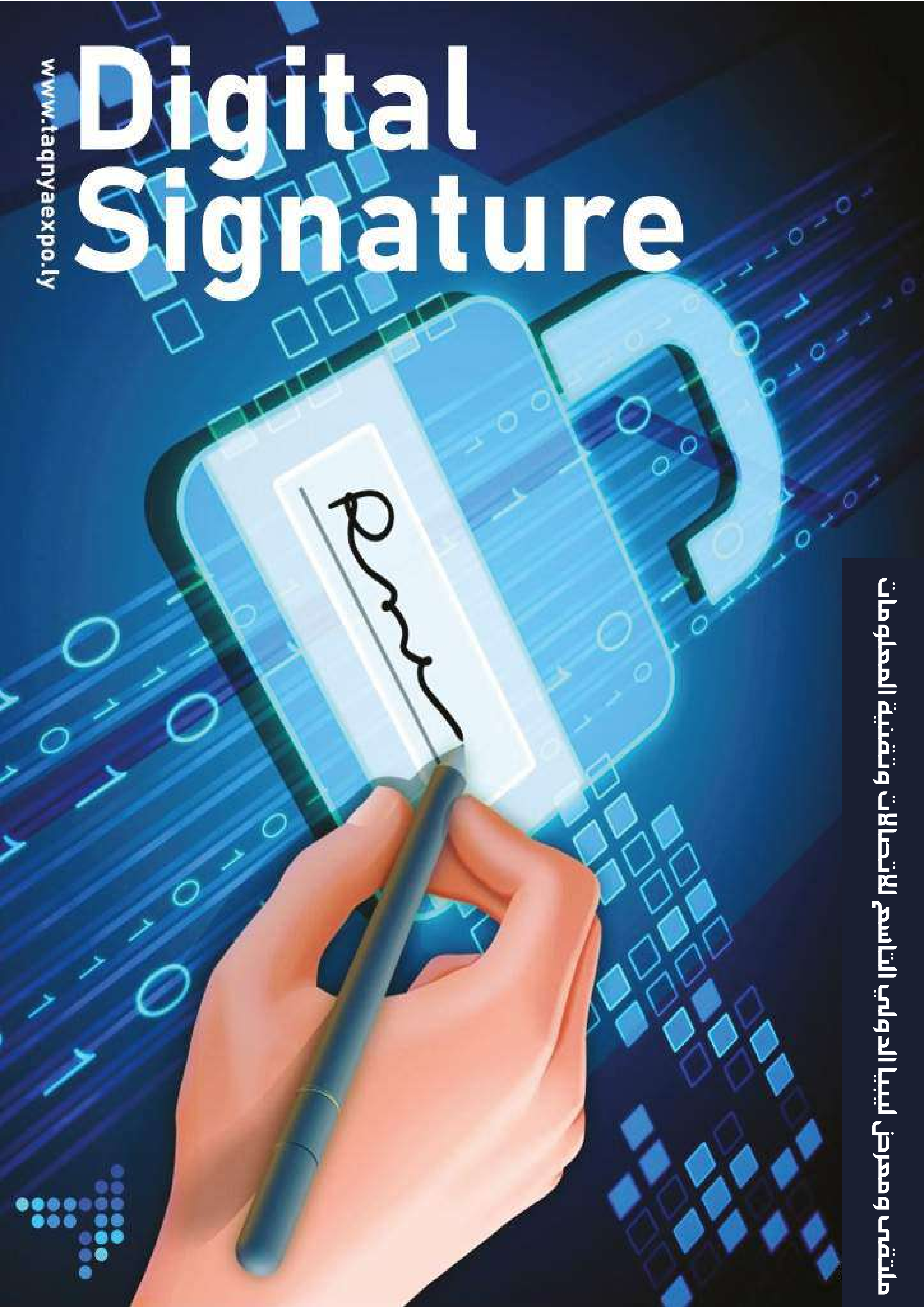
ملتقى ومعرض ليبيا الدولي التاسع
للإتصالات وتقنية المعلومات

The Ninth Libyan International Forum and Exhibition
For Communications and IT

9-12 November

Organized by:

00218 913506666 | www.taqnyaexpo.ly
00218 922104910 | info@taqnyaexpo.ly
00218 0217108380 | info@wahaexpo.com


Digital Signature
www.taqnyaexpo.ly
ملتقى ومعرض ليبيا الدولي التاسع للاتصالات وتقنية المعلومات

TAQNYA

DIGITAL SIGNATURE EXPERT REGISTRATION FORM

FIRST NAME:

LAST NAME:

TELEPHONE: EMAIL

GENDER:
- ☐ MALE
- ☐ FEMALE

AGE:
- ☐ -18
- ☐ 18-30
- ☐ 31-45
- ☐ +45

ACADEMIC QUALIFICATIONS:
- ☐ HIGH SCHOOL DEGREE
- ☐ BACHELOR'S DEGREE
- ☐ MASTER'S DEGREE
- ☐ DOCTORATE'S DEGREE
- ☐ POST DOCTORATE

COMPANY / ORGANIZATION NAME:

TELEPHONE: EMAIL: WEBSITE:

WORKSHOP PRESENTAION BRIEF:
(200 words max)

WAHAEXPO CO.
TRIPOLI INTERNATIONAL FAIR
TRIPOLI- LIBYA
TLF. : +218 91 210 49 10

الواحة للمعارض
WAHAexpo Co.

" التوقيعات الرقمية "

التوقيعات الرقمية هي مفتاح عام أساسي لمصادقة الرسائل. ففي العالم المادي من الشائع استخدام التوقيعات المكتوبة بخط اليد على الرسائل المكتوبة يدويا . ليتم استخدامها لربط الموقع بالرسالة.

وبصورة مماثلة، فإن التوقيع الرقمي هو أسلوب يكرّم الشخص/الكيان للبيانات الرقمية. يمكن التحقق من هذا الربط بشكل مستقل من قبل المتلقي أو من أي طرف ثالث. إذا التوقيع الرقمي هو قيمة تشفير يتم حسابها من بيانات ومفتاح سري معروف فقط من قبل الموقع.

أهمية التوقيعات الرقمية :

من بين جميع بدائل التشفير، يعتبر التوقيع الرقمي باستخدام تشفير المفتاح العام، أداة مهمة ومفيدة للغاية لتحقيق أمن المعلومات.
بصرف النظر عن القدرة على توفير عدم التنصل من الرسائل ، يوفر التوقيع الرقمي أيضًا مصادقة الرسائل وسلامة البيانات.
دعونا نرى بإيجاز كيف يتم تحقيق ذلك من خلال التوقيع الرقمي:-

- مصادقة الرسائل – عندما يتحقق المدقق من صحة التوقيع الرقمي باستخدام المفتاح العام للمرسل ، فإنه يتأكد من أن التوقيع قد تم إنشاؤه فقط من قبل المرسل الذي يطرح المفتاح الخاص السري المقابل وليس أي شخص آخر.

- سلامة البيانات – في حالة تمكن المهاجم من الوصول إلى البيانات وتعديلها ، يفشل التحقق من التوقيع الرقمي في نهاية جهاز الاستقبال. لن تتطابق تجزئة البيانات المعدلة والمخرجات التي توفرها خوارزمية التحقق، وبالتالي يمكن للمتلقي أن ينكر بأمان الرسالة على افتراض أن سلامة البيانات قد تم اختراقها.

- عدم التنصل – نظرًا لأنه من المفترض أن الموقع فقط لديه معرفة بمفتاح التوقيع ، يمكنه فقط إنشاء توقيع فريد على بيانات معينة. ومن ثم إذا نشأ أي نزاع في المستقبل. يمكن للمتلقي تقديم البيانات والتوقيع الرقمي إلى طرف ثالث كدليل.

" Digital Signatures "

Digital signatures are the public-key primitives of message authentication. In the physical world it is common to use handwritten signatures on handwritten letters or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that vines a person/entity to the digital data. This binding can be independently verified by the receiver as well as any third party.
Therefore a Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Importance of Digital Signature:

Out of all cryptographic primitives, the digital signature using the public key cryptography is considered as a very important and useful tool to achieve information security.
Apart from the ability to provide non-repudiation of messages, The digital signature also provides message authentication and data integrity.
Let us briefly see how this is achieved by the digital signature :-

- Message authentication - when the verifier validates the digital signature using the public key of a sender, he is assured that the signature has been created only by the sender who poses the corresponding secret private key and no one else.

- Data integrity – in case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and output provided by the verification algorithm will not match. Hence, the receiver can safely deny the message assuming that data integrity has been breached.

- Non-repudiation– Since it is assumed that only the signer has knowledge of the signature key, he can only create a unique signature on a given data. Thence if any dispute arises in the future. receiver can present data and the digital signature to a third-party as evidence

SPONSORS

الشريك الرسمي

الشركة الليبية للبريد ،الاتصالات وتقنية المعلومات القابضة
Libya Post Telecommunication & IT Holding Company
LPTIC

الراعي الإعلامي

سلام

الراعي الإذاعي

88.
THE TEMPO OF HEART

الراعي الخدمي

المنظمة الليبية
لتقنية المعلومات والاتصالات

الراعي التقني

LibyanSpider

Giga

THANK YOU.

ORGANIZED BY

الواحة للمعارض
WAHAexpo Co.