جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة الثامنة

- هيكلية المفتاح العام PKI(Public Key Infrastructure)
  - ✓ مقدمة
  - ✓ المكونات الأساسية للهيكلية
  - ✓ وظائف الهيكلية
  - ✓ آلية عمل مبسطة للهيكلية

مقدمة إلى هيكلية المفتاح العام
(Public Key Infrastructure(PKI))

- إن أعداد كبيرة من الناس يبيعون و يشترون عبر الانترنت ، وهذا يجعل من الصعب إدارة و ضمان أمن هذه التعاملات باستخدام مفتاح سري (تشفير متناظر)
- ظهرت أهمية البحث عن هيكلية للمفتاح العام عندما أصدرت الحكومة الأمريكية القانون الذي نص على إلغاء الحكومة الورقية و التوجه إلى الحكومة الالكترونية منذ عام 2003
- الهدف من هذه الهيكلية هو :حماية وتوزيع المعلومات المطلوبة في بيئة موزعة على نطاق واسع، حيث يمكن للمستخدمين والموارد وأصحاب المصلحة أن يكونوا في أماكن مختلفة في أوقات مختلفة.
- تزود هذه الهيكلية المتطلبات الأمنية الأساسية الآتية : التكاملية والموثوقية والمصادقة
- تتضمن هذه الهيكلية:
  - ✓ الشهادات الرقمية
  - ✓ التعمية باستخدام المفتاح العام
  - ✓ كيانات مانحة للشهادة من أجل هيكلية أمنية لشبكة واسعة أو شركة

مكونات الأساسية لهيكلية المفتاح العام PKI (1/2)

هيئة إصدار الشهادات (Certification Authority) CA

تمثل حجر الأساس في هذه الهيكلية ، وهي مسؤولة عن كل ما يتعلق بتوليد الشهادات و توقيعها ، وتحتفظ بالمعلومات الدالة على حالة الشهادة (فعالة أو ملغاة)

عملياً هي شركات عالمية موثوقة ومرخص لها بمنح الشهادات الرقمية نذكر منها: **VeriSign**, Let`s Encryption, Entrust, DigiCert, SwissSign, TurkTrust

هيئة التسجيل(Registration Authority) RA

تسجل و تتحقق من طلبات الشهادة المقدمة من قبل المستخدمين و يكون موثوقاً بها من قبل CA إذ تُعلِمُه ليقوم بإصدارها

مكونات الأساسية لهيكلية المفتاح العام PKI (2/2)

➢ **المستودع Repository/ Directory**

يتضمن قاعدة بيانات الشهادات الرقمية الفعالة لـ CA ، كما يوفر البيانات التي تسمح للمستخدمين بتأكد من حالة الشهادات الرقمية للأفراد والشركات التي تتلقى رسائل موقعة رقمياً

➢ **الأرشيف Archive:**

لتخزين وحماية معلومات تكون كافية لتحديد فيما إذا كان ينبغي الوثوق بالتوقيع الرقمي الموجود على وثيقة "قديمة" أو لا

➢ **الشهادات Certifications:**

تتضمن المفتاح العام، ومعلومات عن هوية الكيان الذي يحمل المفتاح الخاص المقابل، و زمن حياة الشهادة، والتوقيع الرقمي الخاص بالـ CA.
قد تحتوي على معلومات أخرى عن الطرف أو المعلومات الموقعة حول الاستخدامات الموصى بها للمفتاح العام.

➢ **المستخدم Users:**

يملك زوج المفاتيح و الشهادة الرقمية

وظائف هيكلية المفتاح العام PKI

➢ **تتمثل وظائف PKI الأكثر شيوعاً في:**

- ✓ إصدار الشهادات
- ✓ إلغاء الشهادات
- ✓ إنشاء قوائم الشهادات الملغاة CRL(Certificate Revocation Lists) ونشرها وتخزينها واسترجاعها
- ✓ إدارة حياة المفتاح
- ✓ تطوير وتحسين وظائف للتحقق من الختم الزمني
- ✓ التحقق من صحة الشهادة

آلية عمل الـ PKI (1/6)

١. تقوم هيئة التسجيل (RA) بتسجيل طلبات الحصول على الشهادات و التحقق من هذه الطلبات

٢. تقوم هيئة إصدار الشهادات (CA) بإنشاء و توزيع الشهادات

٣. تقوم هيئة التحقق من الفعالية الـ (Authority of validation) AV بالتحقق من فعالية الشهادات

٤. في كل لحظة، يقوم مخزن قائمة الشهادات الملغاة CRL بإدارة حالة الشهادات و ذلك للأخذ بالحسبان الشهادات التي أصبحت ملغاة

٥. تنشر الشهادات و تخزن ضمن مستودع الشهادات (directory)

آلية عمل الـ PKI (2/6)

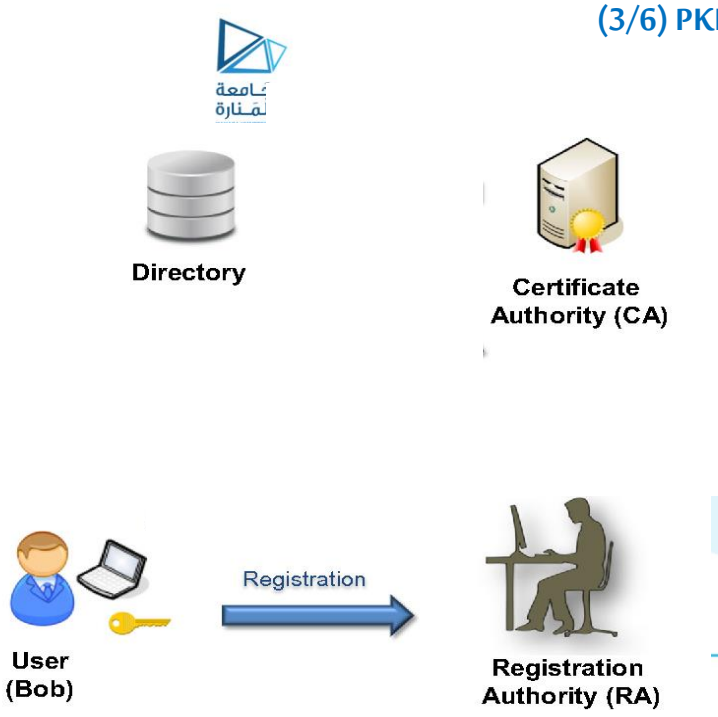
Directory

Certificate Authority (CA)

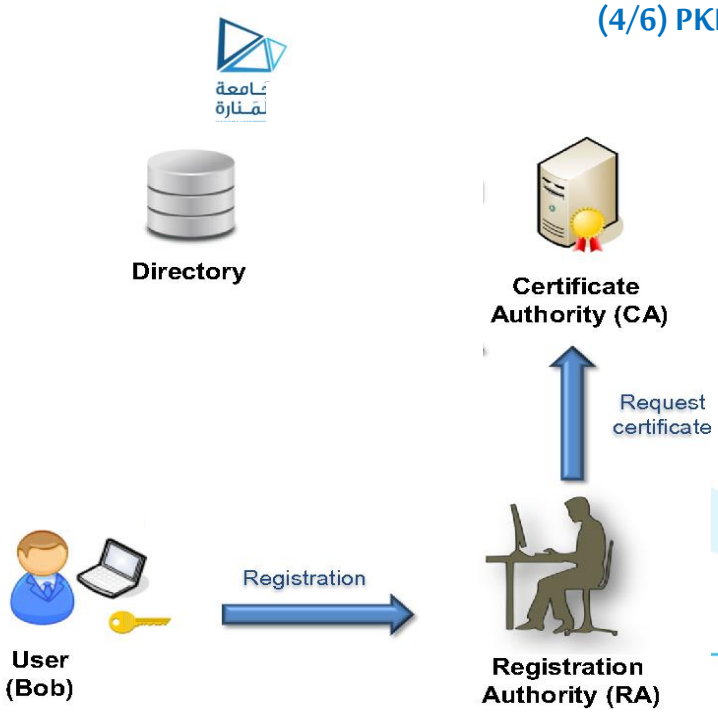
User (Bob)

Registration Authority (RA)

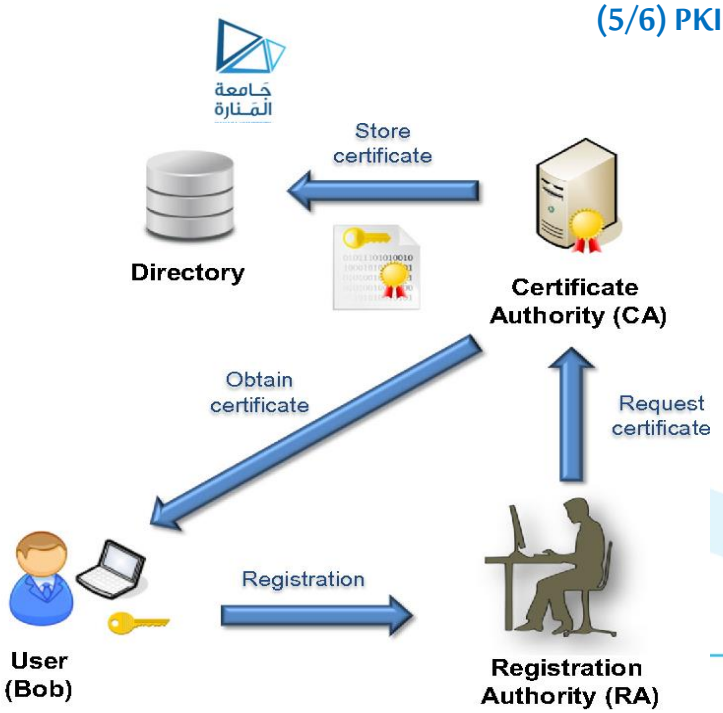
آلية عمل الـ PKI (3/6)



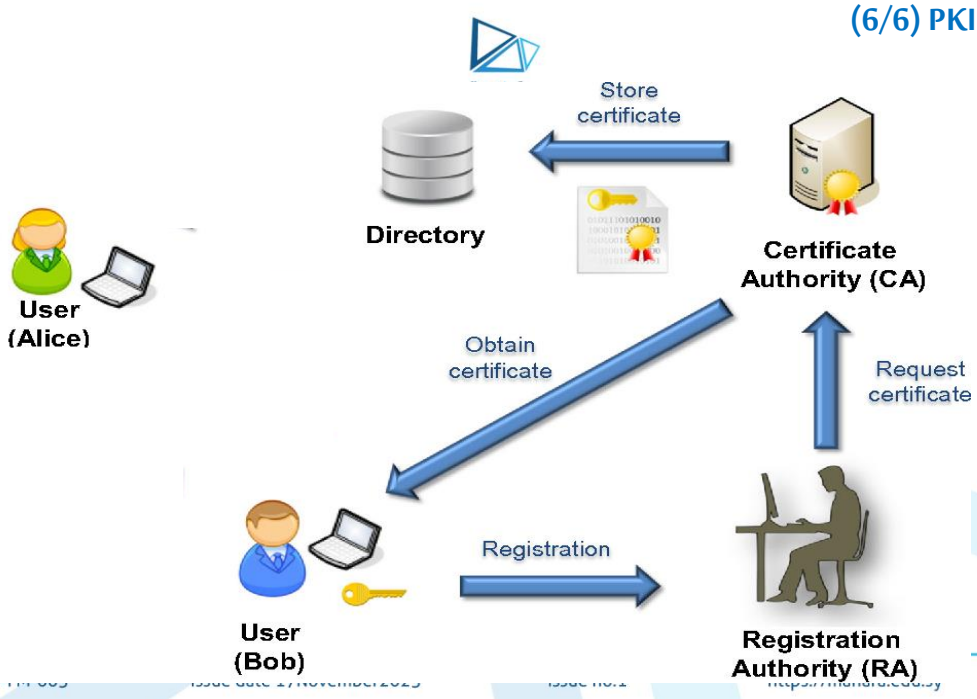
آلية عمل الـ PKI (4/6)



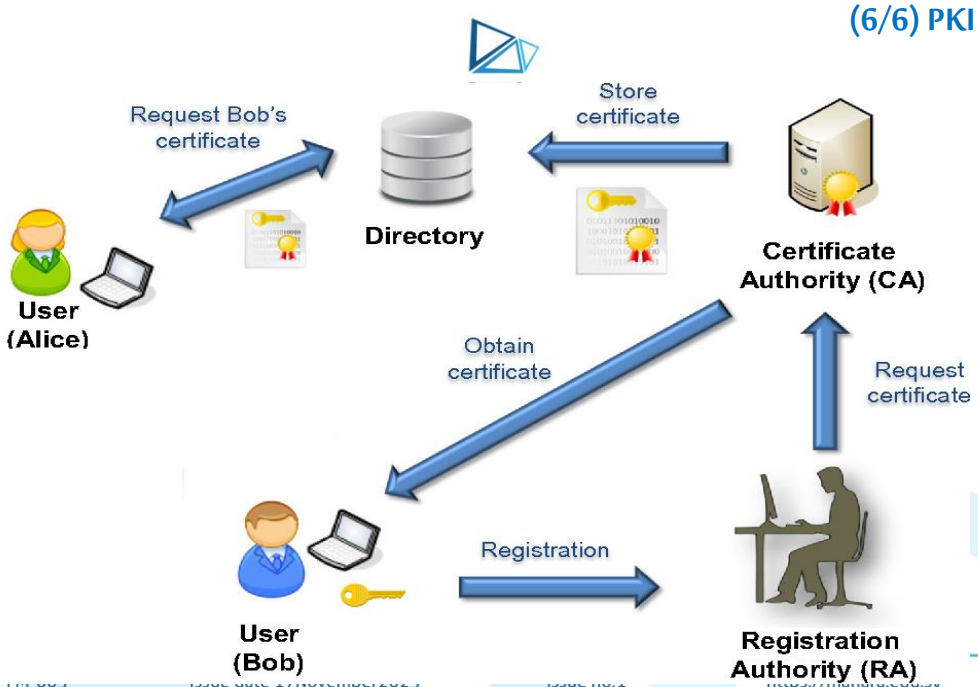
آلية عمل الـ PKI (5/6)



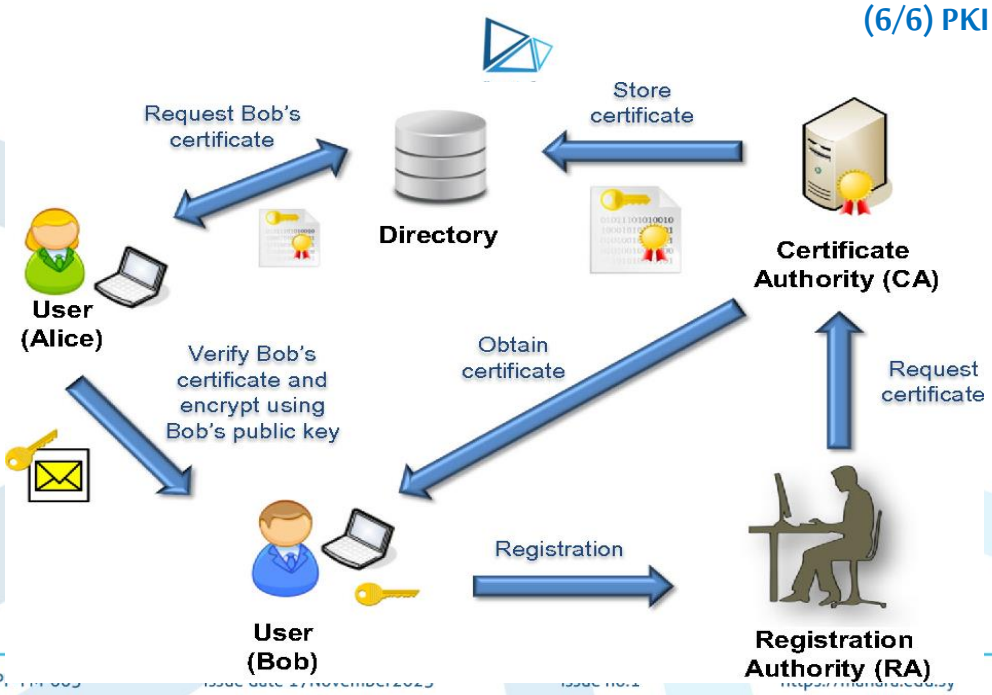
آلية عمل الـ PKI (6/6)



آلية عمل الـ PKI (6/6)



آلية عمل الـ PKI (6/6)



جَـامعة
المَـنارة
MANARA UNIVERSITY

نهاية المحاضرة