دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

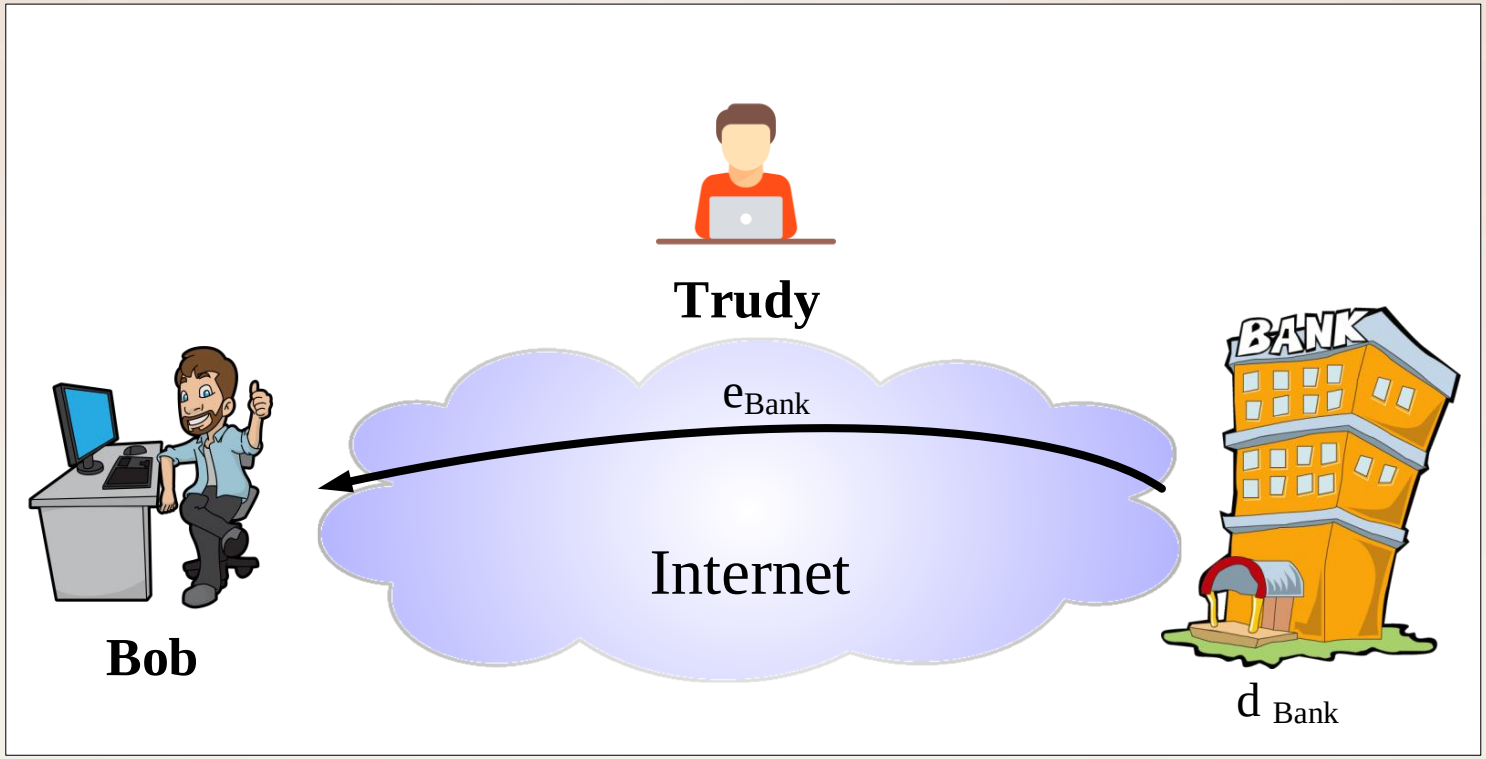
PKI

نستوه طاهری جوان

nastooh@aut.ac.ir

زیرساخت کلید عمومی

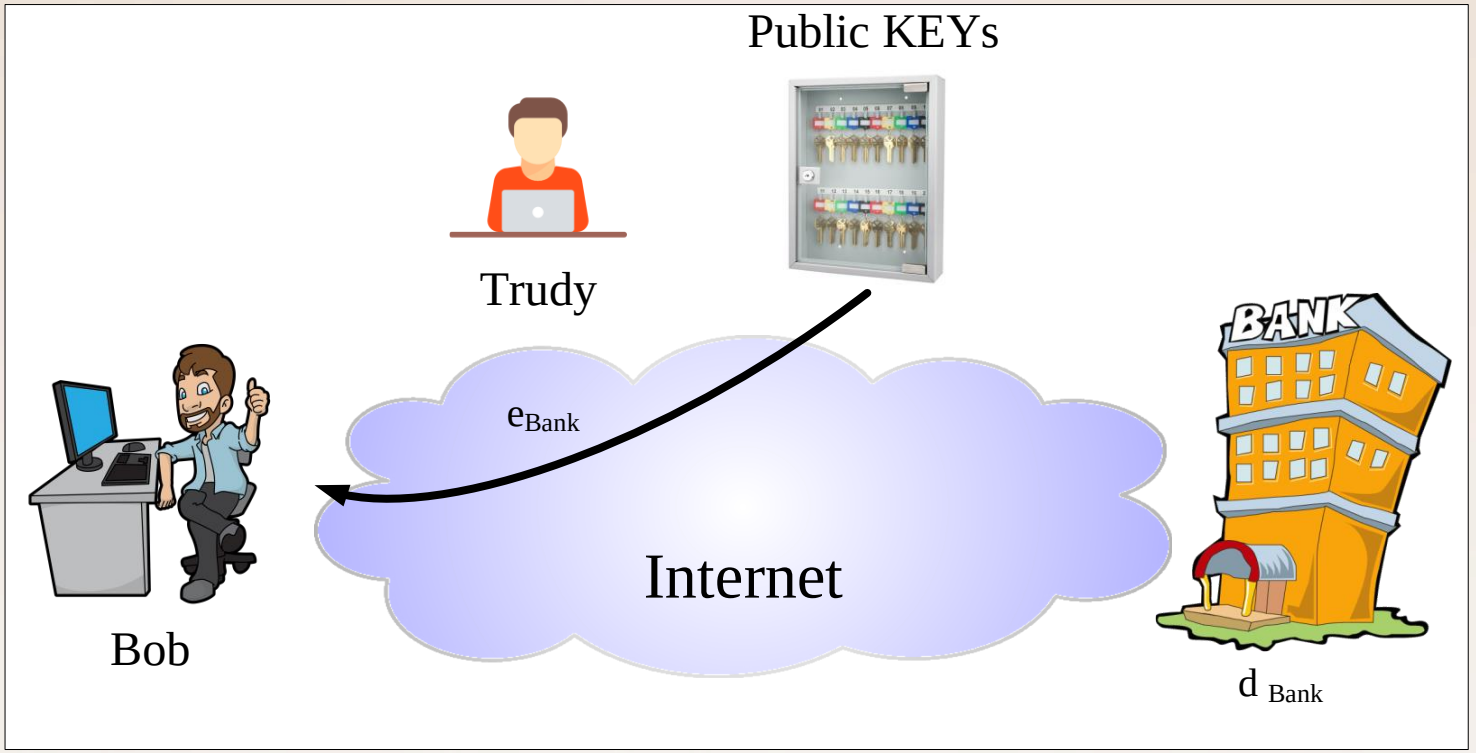
- ✓ مشکل بزرگ PKC
  - ○ نیاز به اعتبار سنجی کلیدهای عمومی



شکل برای توضیح شفاهی

زیرساخت کلید عمومی

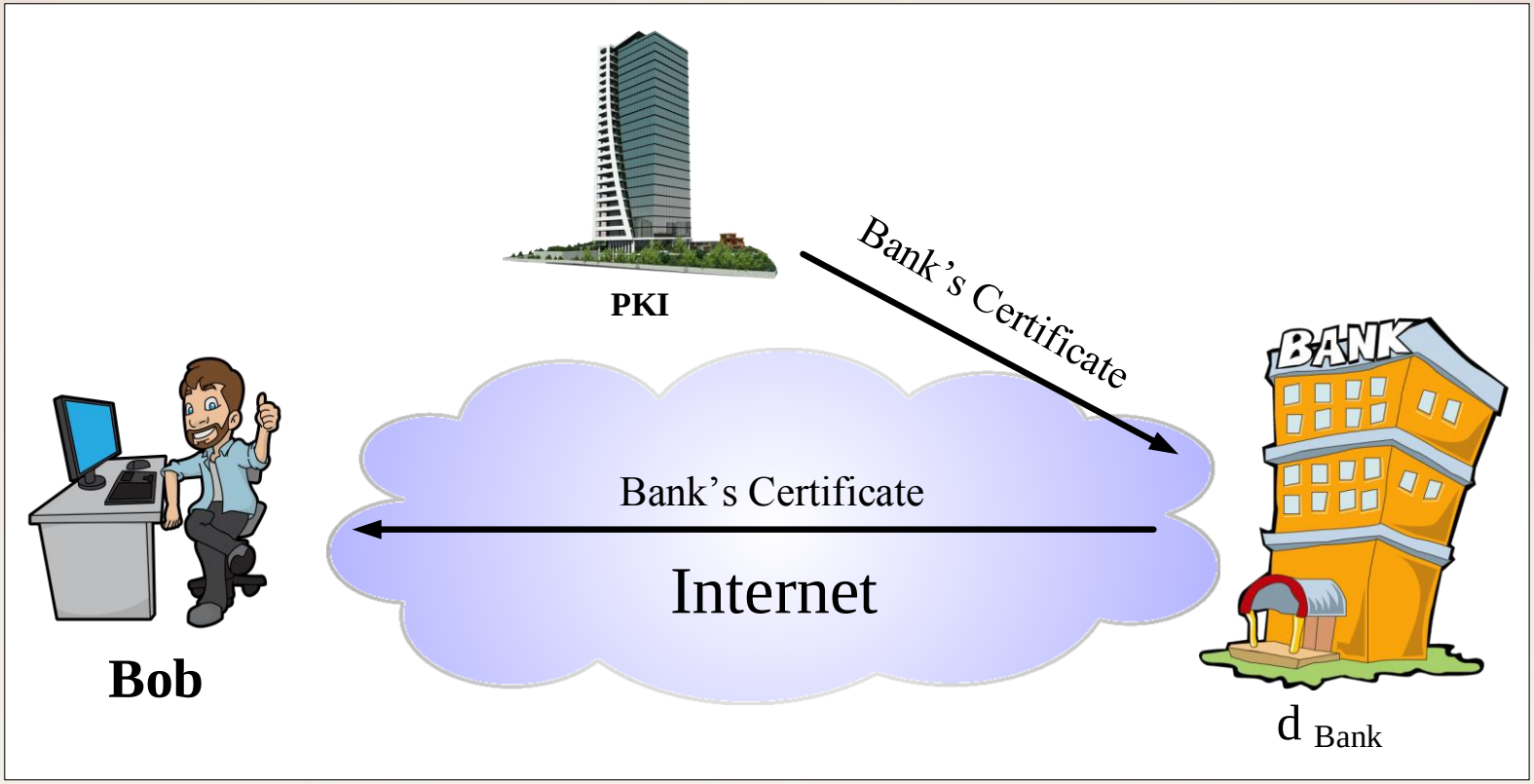
- ✓ مشکل بزرگ PKC
  - ○ نیاز به اعتبار سنجی کلیدهای عمومی



شکل برای توضیح شفاهی

زیرساخت کلید عمومی

- ✓ راه کار اولیه



شکل برای توضیح شفاهی

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راه کار اولیه
  - دریافت گواهینامه از PKI توسط بانک
    - به زبان ساده، گواهینامه حاوی کلید عمومی بانک است که یک امضای دیجیتال از PKI پای آن خورده است.
  - ارسال گواهی نامه توسط بانک برای هر مشتری
  - اعتبار سنجی گواهینامه توسط مشتری ها
    - برای این کار به کلید عمومی PKI نیاز است...
  - استفاده از کلید عمومی بانک، پس از اعتبار سنجی گواهی نامه

آیا مشکل حل شد؟

مشتری بانک (طرف دوم ارتباط)، این بار کلید عمومی PKI را از کجا بدست آورد؟

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راه کار اولیه

- ○ تنها راه باقی مانده:

قرار دادن کلید عمومی PKI، به روشی مطمئن در سیستم عامل (مثلا مرورگر ها) از قبل

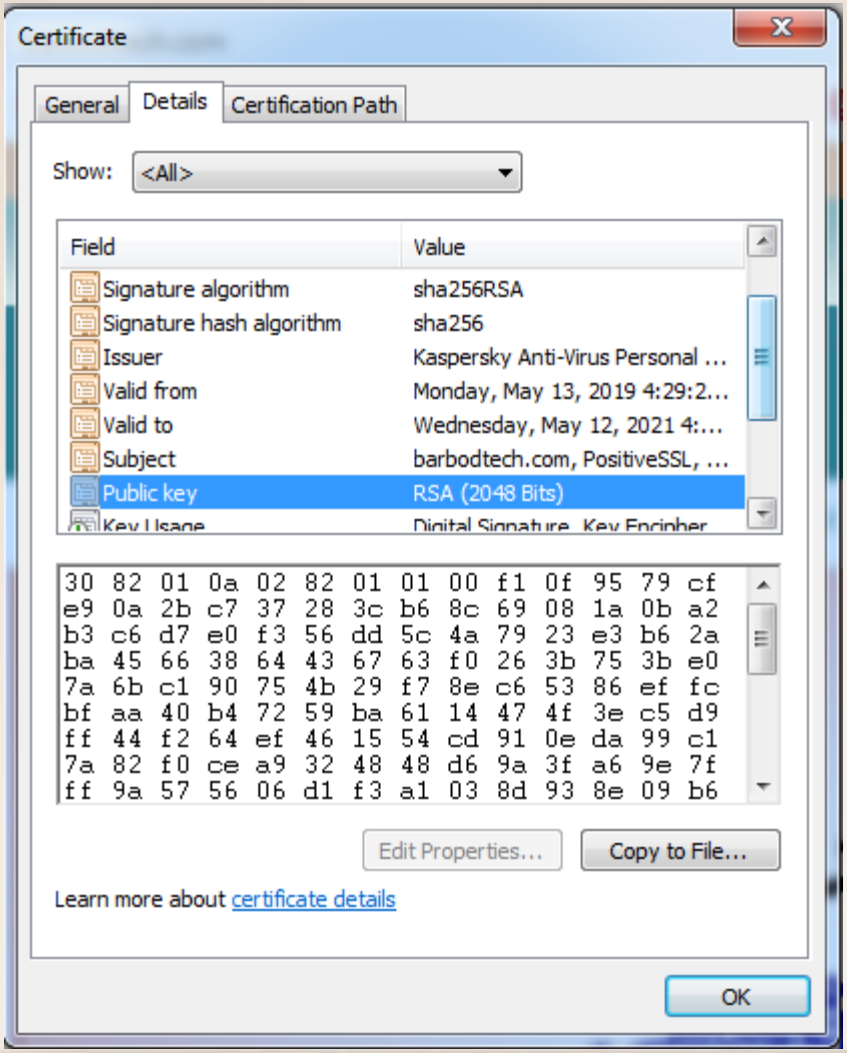
زیرساخت کلید عمومی

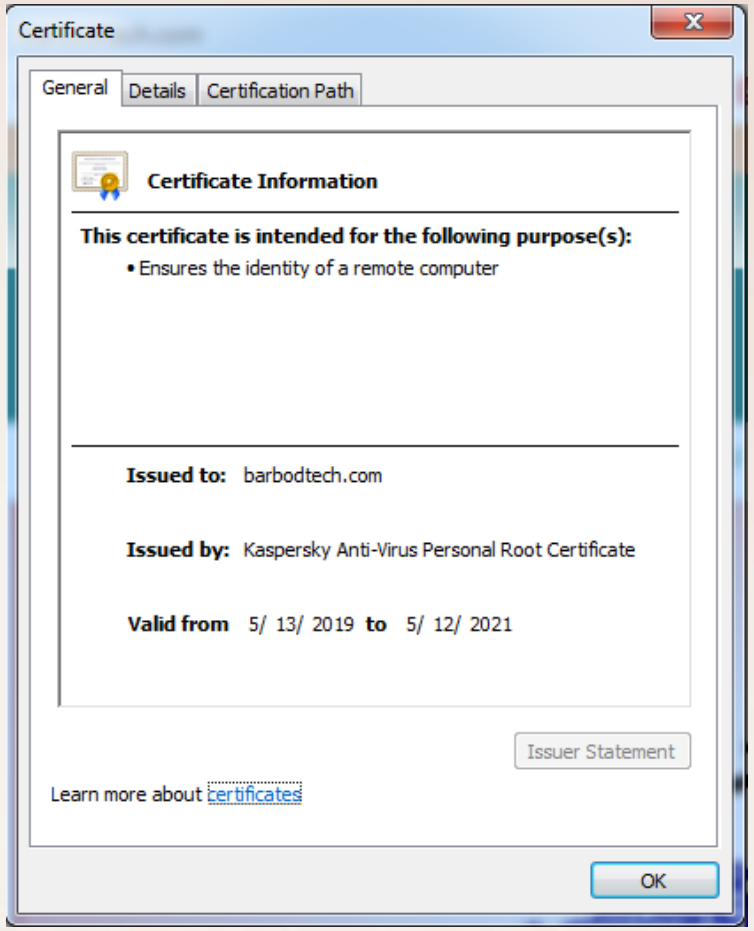
- ✓ یک گواهینامه ی نمونه
  - یک گواهی نامۀ فرضی می تواند شامل فیلدهای زیر باشد:

Serial Number: xx00000000123
Name: Nastooh Bank
Email: info@nastooh.bank
Address: Tehran, IRAN.
Valid from: 21 may 2018, 12:17:57
Valid to: 21 may 2020, 12:17:56
Issued By: CA X625
Public Key: xxxxxxxxxxx
Digital Signature: xxxxxxxxx

زیرساخت کلید عمومی

✓ یک گواهینامه ی نمونه





زیرساخت کلید عمومی

✓ سوال های مهم

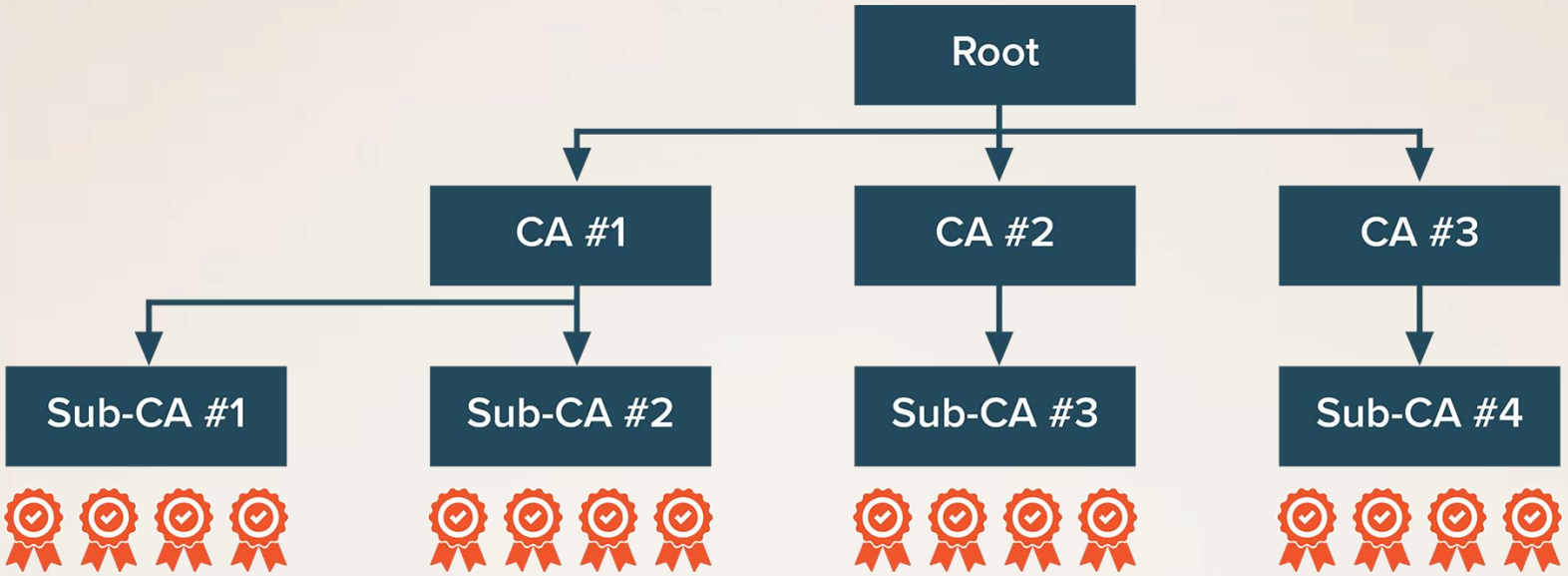
- آیا PKI فقط یک مرکز است؟
  - آیا فقط یک مرکز با یک کلید عمومی-خصوصی گواهی صادر می کند؟
    - بحث Single pint of Failure چه می شود؟
    - بحث لود کاری؟
  - آیا می توان مراکز متعددی داشت که همگی با یک کلید عمومی-خصوصی کار کنند؟
    - بحث مسئولیت خطاها و خرابکاری احتمالی چه می شود؟
  - آیا می توان مراکز متعددی داشت که هر مرکز با کلید-عمومی خصوصی خود کار کند؟
    - تمام این کلیدهای عمومی باید در مرورگرها از پیش وجود داشته باشند؟

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI

یک ساختار چند سطحی



nastooh@aut.ac.ir

زیرساخت کلید عمومی

✓ راهکار نهایی در PKI

- هر سطح، برای سطح پایین تر گواهینامه صادر می کند.
- هنگام برقراری یک ارتباط، طرف اول باید علاوه گواهینامهٔ خود، باید دنباله ای از گواهینامه ها را برای طرف دوم ارسال کند.
  - به این دنباله معمولا زنجیرهٔ اعتماد، یا مسیر گواهینامه گویند!
- فقط نیاز به وجود کلید عمومی ریشه در مرورگر طرف دوم است.
  - آیا در دنیا فقط یک ریشه وجود دارد؟
- طرف دوم، پس از دریافت دنباله ای از گواهینامه ها، از انتها گواهینامه ها و کلیدهای عمومی را اعتبار سنجی می کند، تا به کلید عمومی طرف اول برسد.

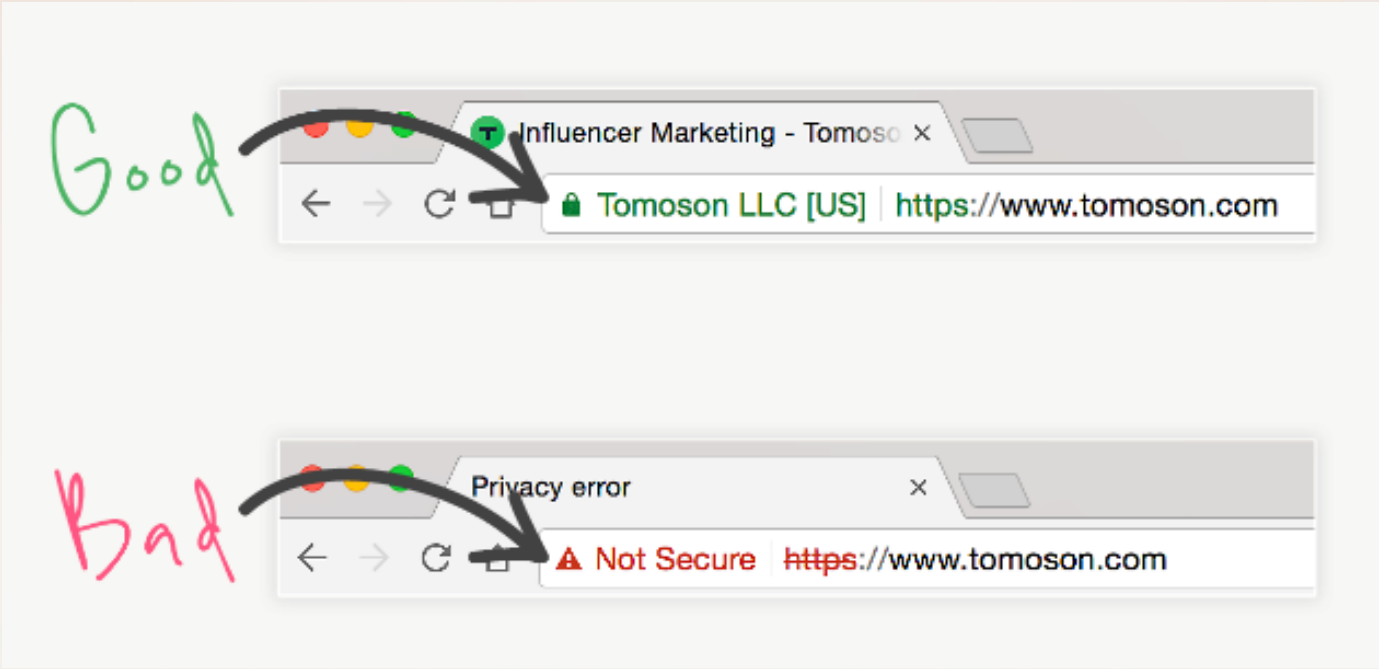
در واقع عملکرد PKI بر این اصل استوار است که همهٔ افراد به ریشه اطمینان دارند و کلید عمومی ریشه را به گونهٔ امنی در اختیار دارند!

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI

تفاوت سایت با زنجیرهٔ اطمینان و بدون زنجیرهٔ اطمینان در غالب مرورگر ها

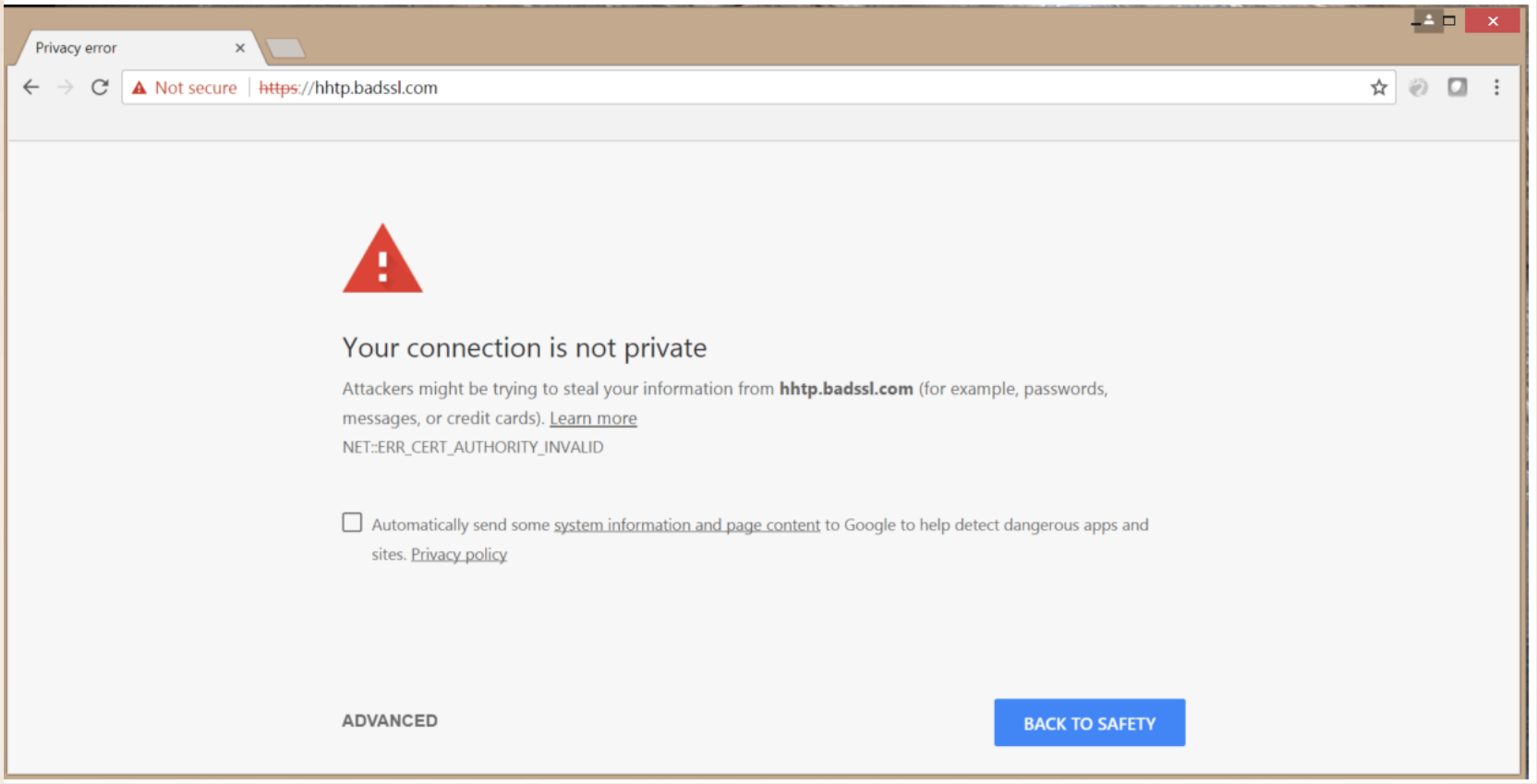


nastooh@aut.ac.ir

زیرساخت کلید عمومی

✓ راهکار نهایی در PKI

پیغام هشدار مرورگر هنگام ویزیت یک سایت بدون زنجیرهٔ اطمینان معتبر



nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI
  - نکات جانبی
    - می توان CAهای جدید تاسیس کرد.
    - می توان یک گواهینامه را پس از صدور، باطل کرد. (به سختی)
    - واقعا در دنیا چندین ریشه برای PKI داریم. (حدود صد عدد)
      - مانند Verisign، Cacert، GoDaddy و و و
    - شرکت های تولید کننده مرورگر (یا نرم افزارهای دیگر) باید به گونه ای محصول خود را طراحی کنند که نیازی به دریافت کلیدهای عمومی ریشه(ها) از بیرون نباشد و به صورت پیش فرض در نرم افزارها وجود داشته باشند!
    - مرورگرها اگر برای اعتبارسنجی زنجیرهٔ اعتماد به مشکل بخورند، با پیغامهای خاص و هشداردهنده، از کاربر کسب تکلیف می کنند.

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI
  - سوال مهم: چه کسی باید اقدام به تاسیس CA کند؟
    - افراد عادی؟
    - قوه های قضائیه یا وزارت های دادگستری؟
    - گروه های مدنی؟
    - کانون های وکلا؟
    - ...
  - رویکردهای عمومی مردم در کشورهای مختلف، در برابر سوال فوق متفاوت است.

عموما ریشه ها برای خود شعباتی در دنیا تاسیس میکنند و به این ترتیب ساختار سلسله مراتبیِ PKI تشکیل می شود.

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI
  - پس از پیاده سازی PKI و گواهینامه های آن، کاربردهای متنوعی برای آن می توان متصور شد.

- ارتباطات امن از طریق وب، مثل:
  - رد و بدل کردن پسوردها و سایر اطلاعات محرمانه برای حساب های کاربری اینترنتی، مانند:
    - « اکانت های ایمیل
    - « بانکداری اینترنتی
- امضای قراردادهای الکترونیکی
- امضای چک های الکترونیکی

nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI
  - ابطال گواهینامه ها
    - آیا می توان زودتر از موعد، یک گواهی نامه را (به هر دلیلی) باطل کرد؟
      - مثلا بحث کلاه برداری مطرح شود.
      - یا کلید خصوصی یک نفر لو رفته و خواهان ابطال گواهینامه قبلی باشد.
    - اما چگونه این ابطال را در اسرع وقت و طور مطمئنی به اطلاع تمام دنیا برسانیم؟؟!!

زیرساخت کلید عمومی

- ✓ راهکار نهایی در PKI
  - ابطال گواهینامه ها
    - استفاده از CRL (Certification Revocation List)
      - هر CA باید به طور منظم و متناوب، مثلا هفتگی یا حتی روزانه، لیستی از گواهینامه هایی که باطل شده اند (نه منقضی ها، چرا؟)، منتشر کند.
      - کاربران موظفند قبل از استفاده از یک گواهینامه، ابتدا CRL را دانلود کرده و چک کنند.
      - سوال: در زمان بین دو انتشار CRL تکلیف چیست؟
      - در کل این روش به قدر کفایت سریع نیست.
    - استفاده از OCSP (Online Certificate Status Protocol)
      - یک وب سرویس آنلاین که تمام گواهینامه های باطل شده را جمع آوری میکند.
      - کاربران باید پس از اعتبار سنجی زنجیرهٔ اعتماد، سریعا از OCSP استعلام آنلاین بگیرند.
      - OCSP در عمل به صورت توزیع شده پیاده سازی شده است.

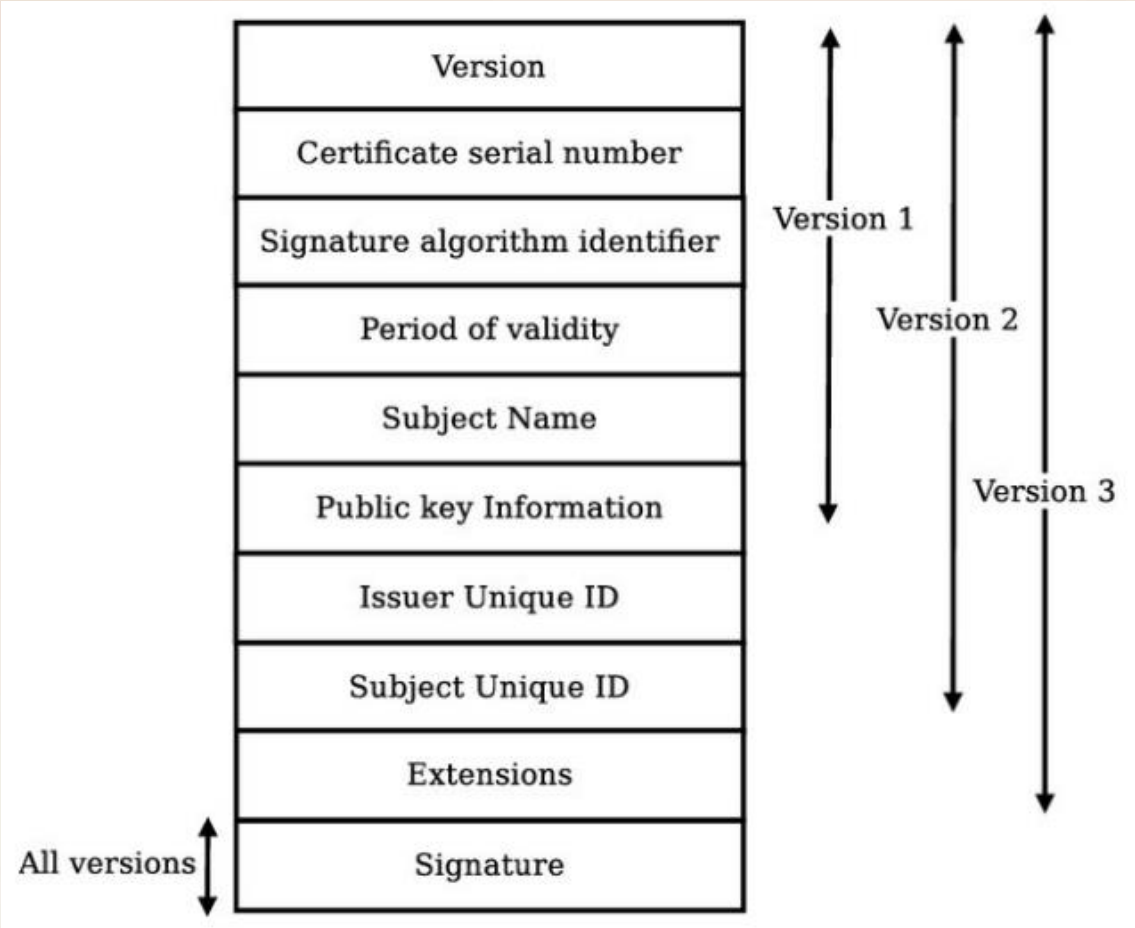
nastooh@aut.ac.ir

زیرساخت کلید عمومی

- ✓ استاندارد X.509
  - ارائه شده در سال ۱۹۸۸
  - دارای سه نسخهٔ بهبود یافته تا امروز
  - نحوهٔ نامگذاری ها و پر کردن فیلدها، دارای استاندارد است.

زیرساخت کلید عمومی

- ✓ استاندارد X.509



فرمت گواهینامه ها

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان