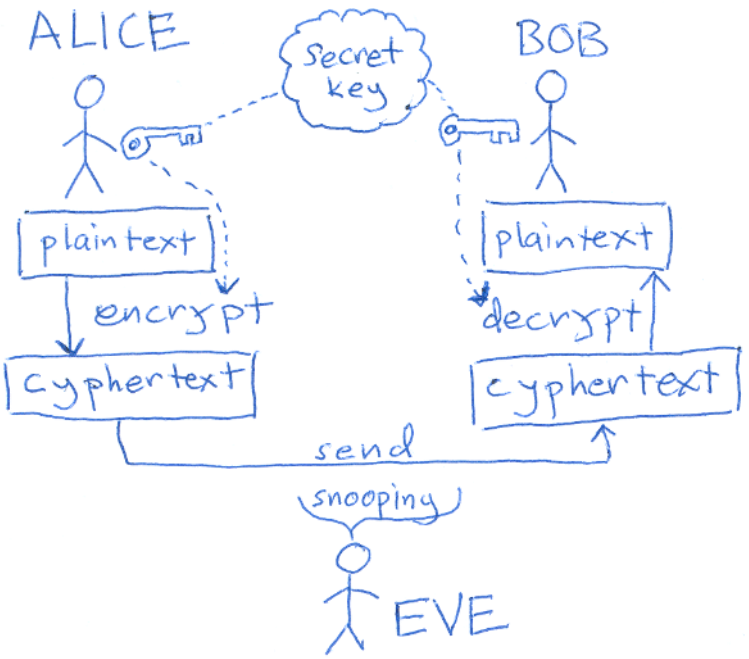


RFID Security

Implementation of Security and Cryptography in RFID \ NFC Systems

121/3 Bar-Kochba St., Herzliya 46440 Israel 46440 בר כוכבא 121/3 הרצליה
+972.54.7504430 daniel@rfidgen.com

Topics

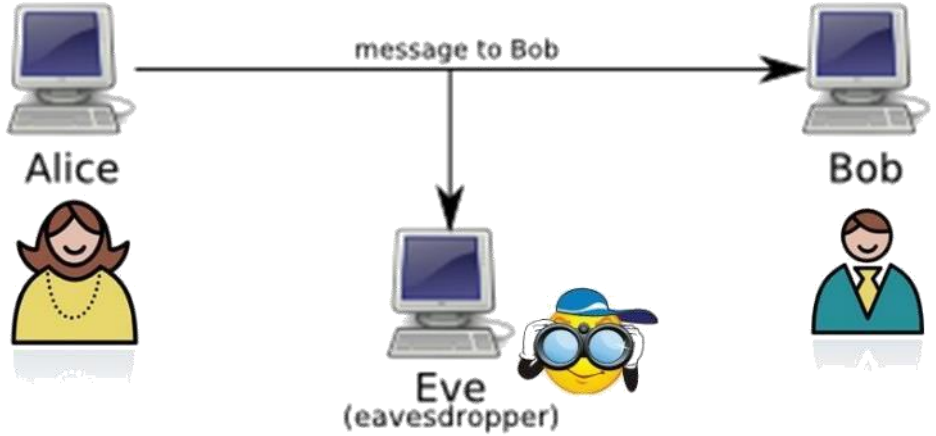
- Introduction:
  - Bob and Alice
  - History
  - Kerckhoffs principle
- Symmetric VS. Asymmetric
  - Explanation
  - Which is better
  - What NSA says?
- RFID Frequencies and apps
  - Frequencies, standards, types
- Security In RFID
  - Authentication
  - ID or Credential
  - Use Cases:
    - Access Control
    - Passports
    - Credit Cards
    - Public Transport
    - Consumables Protection
    - Extending RFID to electronics
    - NFC – deployment and clearing transactions

Introduction

121/3 Bar-Kochba St., Herzliya 46440 Israel 46440 הרצליה 121/3 בר כוכבא
+972.54.7504430 daniel@rfidgen.com

Alice, Bob and (evil) Eve

- Alice and Bob want to communicate securely.
- A attempt to communicate in plain text, will be tampered by evil Eve.
- Cyphered communication requires to establish a key between Alice and Bob !!



Introduction – History

- **1900 BC** Circa, Egypt – Rudimentary letter substitutions.
- **1500 BC** Mesopotamia – Encrypted recipes for pottery glaze.
- **600 BC** "abtash" cypher used by Hebrews
- **800 AD** – Al-Kindi, an Arab mathematician writes "*Manuscript for the Deciphering Cryptographic Messages*"
- **1587** Mary, Queen of Scots is executed following the decryption of a cyphered message involving her in the Babington plot during the reign of Queen Elizabeth I

http://en.wikipedia.org/wiki/History_of_cryptography

Introduction (2)

- Mathematician Marian Rejewski, at Poland's Cipher Bureau, in December **1932** deduced the detailed structure of the German Army Enigma (**Not the Brits!!**)
- On **25 July 1939**, at Warsaw, Polish officers initiated French and British intelligence representatives into the secrets of Enigma decryption.
- At the end of the War, on **19 April 1945**, Britain's top military officers were told that they could never reveal that the German Enigma cipher had been broken because it would give the defeated enemy the chance to claim they "***were not well and fairly beaten***"

http://en.wikipedia.org/wiki/History_of_cryptography

Post WW II Cryptography

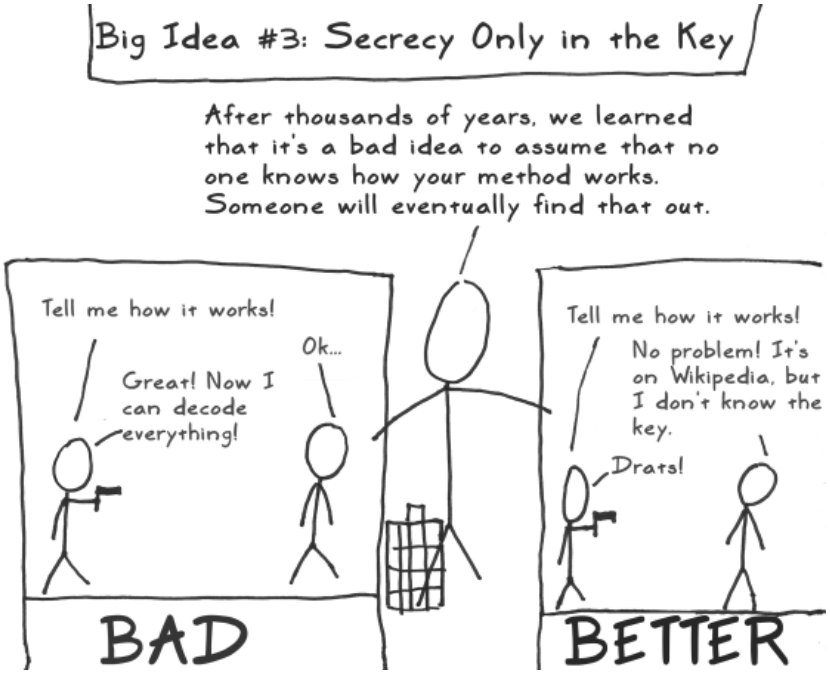
- In **1952**, the US Government recognizes the importance of Cryptography and founds the National Security Agency – NSA
- Mid **1970s** – DES (Data Encryption Standard) was submitted by IBM, for the National Bureau of Standards (now NIST) in order to allow secure electronic communication for banks and large financial organizations.
- **1977** – Adopted and published as a Federal Information Processing Standard (currently at FIPS 46-3) (*thank you NSA*)
- **1976** – Whitfield Diffie and Martin Hellman publish the principles of Public Key Cryptography and introduced a **radically new method of distributing cryptographic keys.**
- **2001** – aging DES is officially replaced by the Advanced Encryption Standard (AES) by NIST (FIPS 197)

http://en.wikipedia.org/wiki/History_of_cryptography

Kerckhoffs' principle

1883, Auguste Kerckhoffs, *La Cryptographie Militaire*he

The System shall not require secrecy, and it should not be a problem if it falls into enemy hands;



How up to date is Kerckhof's principle?

2008: London's Oyster card has been cracked, and the final details will become public in October

October 21, 2014:

Android NFC hack allow users to have free rides in public transportation.

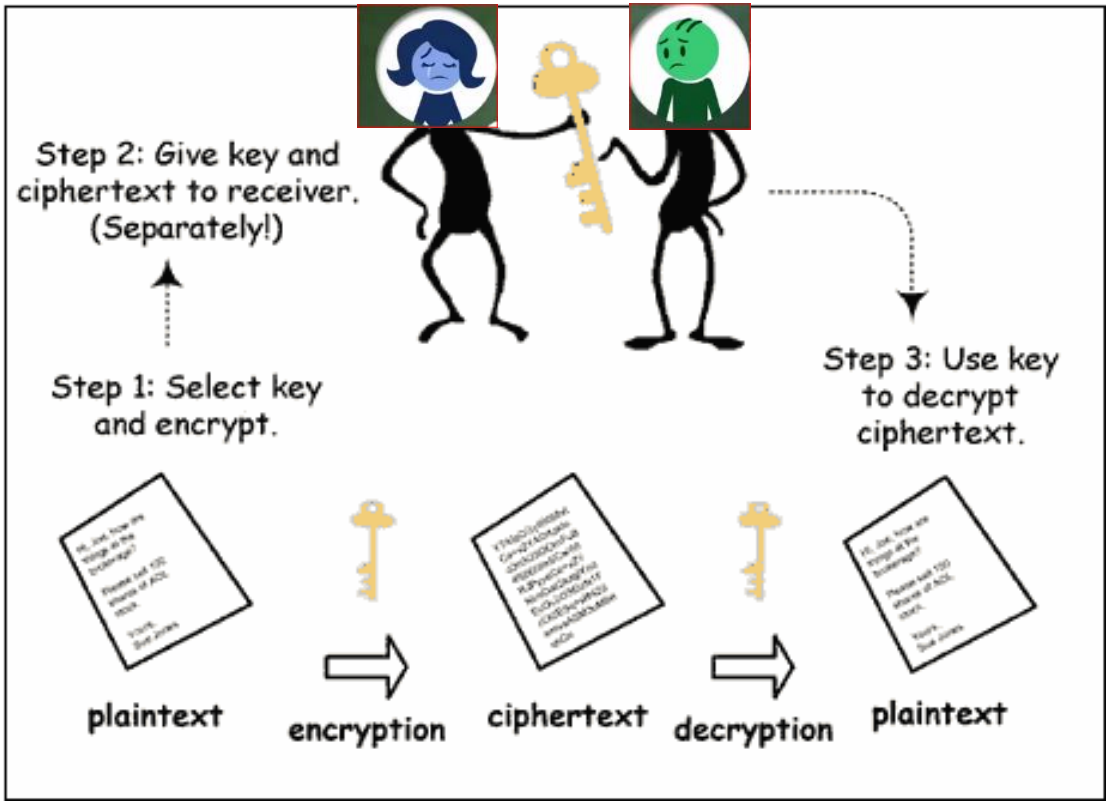
"Secrecy is fragile. *Mifare Classic*'s security was based on the belief that no one would discover how it worked"

Gen ID Technologies Ltd

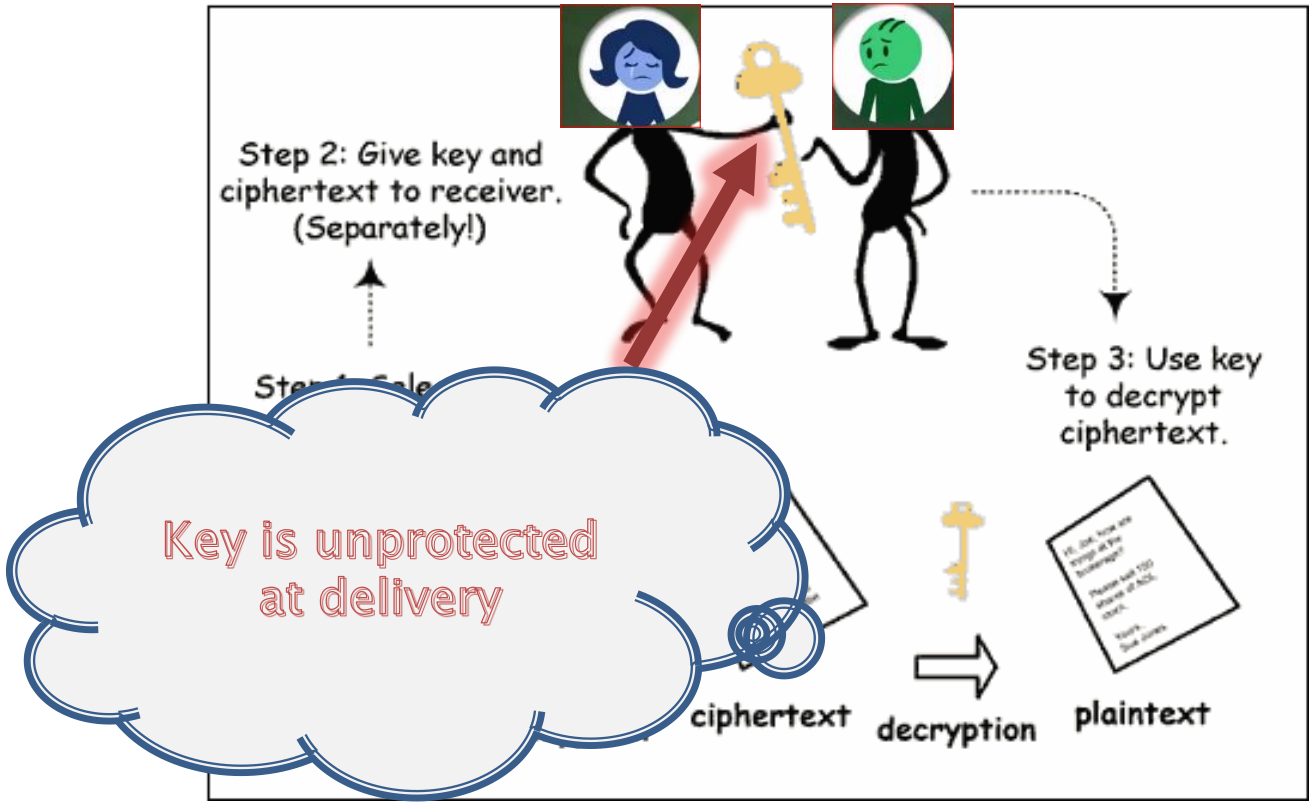
Symmetric VS. Asymmetric Cryptography

121/3 Bar-Kochba St., Herzliya 46440 Israel 46440 הרצליה 121/3 בר כוכבא
+972.54.7504430 daniel@rfidgen.com

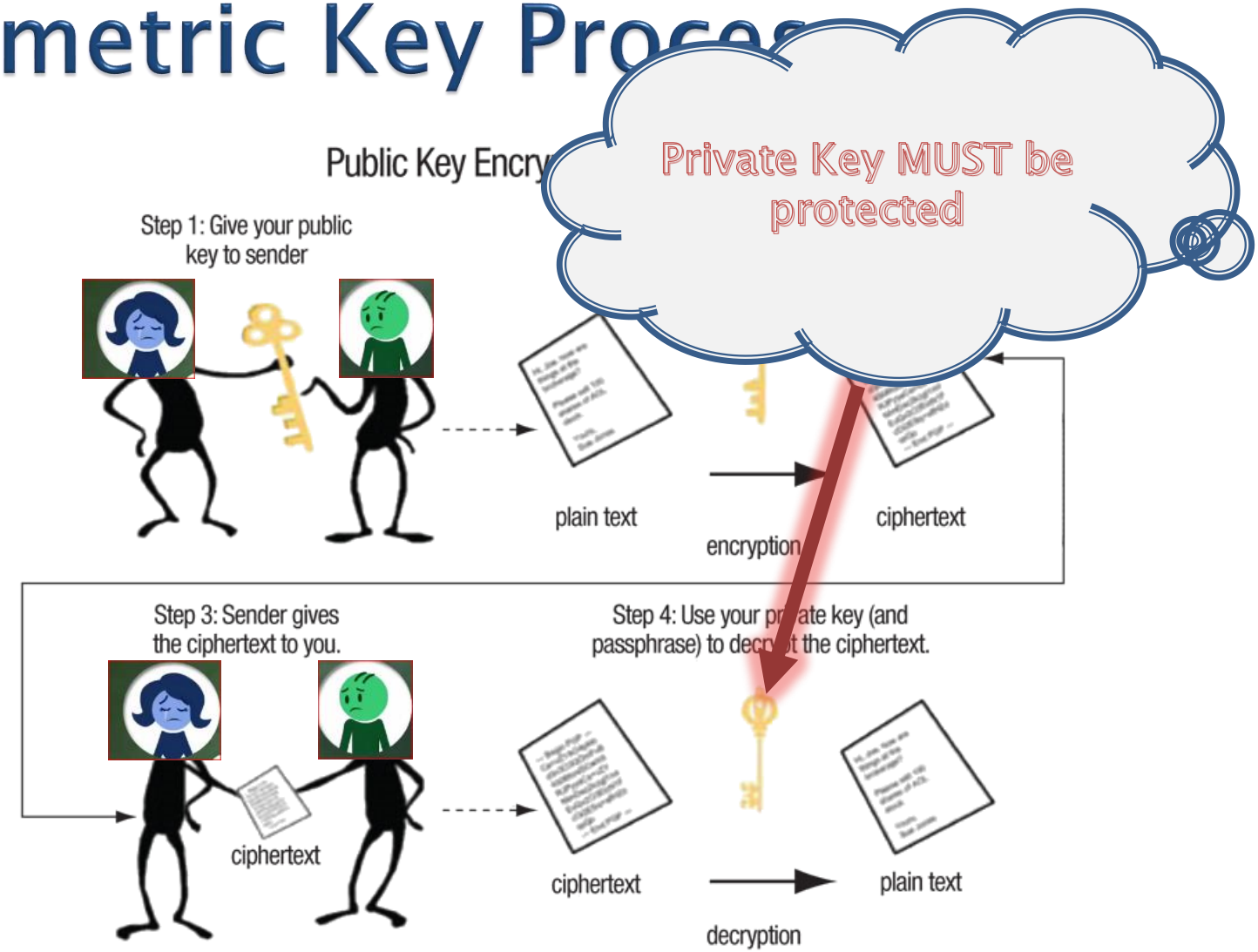
Symmetric Key Ecosystem



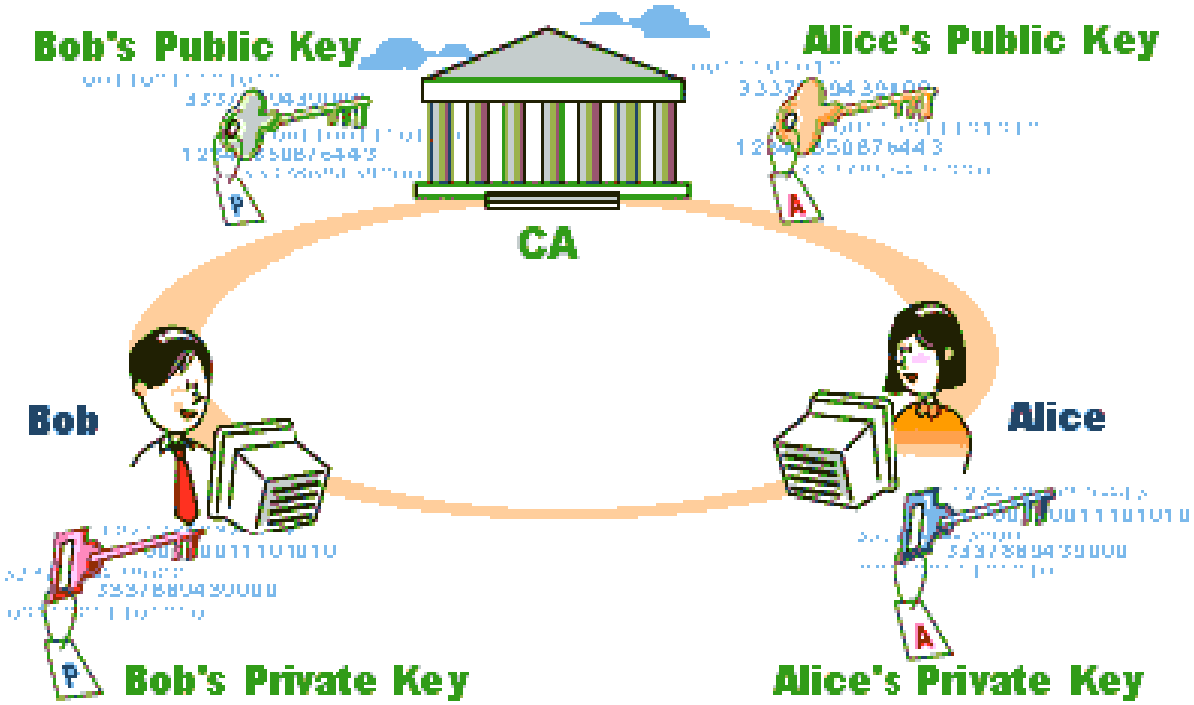
Symmetric Key Ecosystem

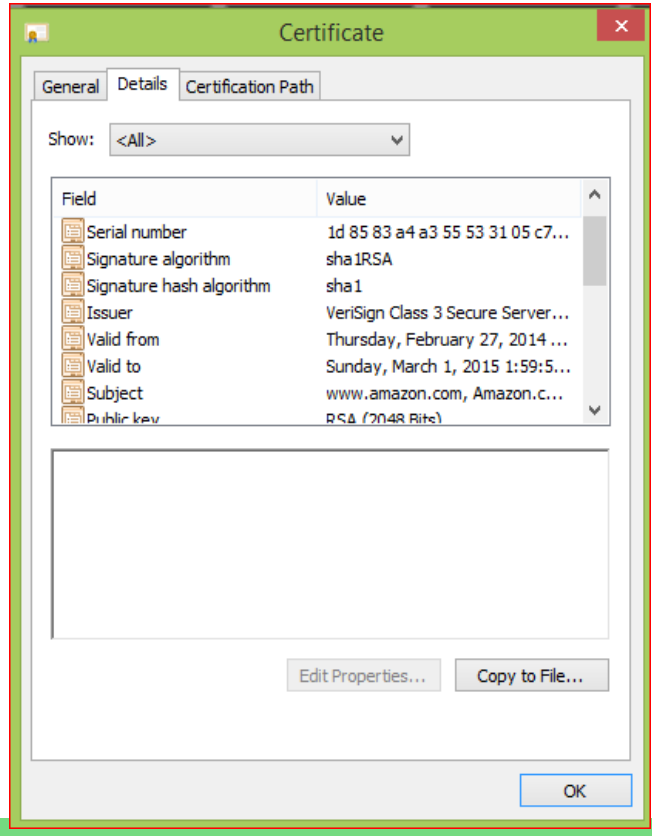


Asymmetric Key Proces



Public Key Infrastructure – PKI





Gen ID Technologies Ltd

Symmetric or Asymmetric – Summary

Asymmetric

1) Alice and Bob agree on a public-key cryptosystem
2) Bob sends Alice his public key
3) Alice encrypts her message using Bob's public key and sends it to Bob
4) Bob decrypts Alice's message using his private key

Symmetric

1) Alice and Bob agree on a cryptosystem
2) Alice and Bob agree on a key
3) Alice takes her plaintext message and encrypts it using the encryption algorithm and the key.
4) Alice sends the ciphertext message to Bob
5) Bob decrypts the ciphertext message with the same algorithm and key

Which is better ?

Symmetric

- Keys must be distributed **in secret**
- If a key is compromised, Eve (eavesdropper) can
  - decrypt any message
  - pretend to be one of the parties
- A network requires a great number of keys

Asymmetric

- **slow (~1000 times slower than the symmetric)**
- vulnerable to chosen-plaintext attacks

How do we solve these problems?

- Hybrid Cryptosystems
  1) Bob sends Alice his public key.
  2) Alice generates a ***random symmetric session key***, encrypts it using Bob's public key, and sends it to Bob.
  3) Bob decrypts Alice's message using his private key to recover the ***session key***.
  4) Both of them encrypt their communications using the same (Symmetric) ***session key***.

Other workarounds

- Benett and Brassard proposed a protocol for a secret key exchange between Alice and Bob in 1984 (BB84) – http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols
- Use Key diversification:

  Div_Key = f (Unique_ID, Master_Key)
- Use Secure Elements (**SE**) or Secure Access Modules (**SAM**) to store your keys and provide Cryptographic Services.
- Use signatures to sign your data
- Use Key Rolling Mechanism

NSA Position on AES Keys

Suite B Cryptography

Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting National Security Systems (NSS). Suite B includes cryptographic algorithms for encryption, key exchange, digital signature, and hashing.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Encryption	FIPS Pub 197	128 bit keys for SECRET 256 bit keys for TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH)	Key Exchange	NIST SP 800-56A	Curve P-256 for SECRET Curve P-384 for TOP SECRET
Elliptic Curve Digital Signature Algorithm (ECDSA)	Digital Signature	FIPS Pub 186-4	Curve P-256 for SECRET Curve P-384 for TOP SECRET
Secure Hash Algorithm (SHA)	Hashing	FIPS Pub 180-4	SHA-256 for SECRET SHA-384 for TOP SECRET

PER CNSSP-15 (SEC.8), THE QUALITY OF THE CRYPTOGRAPHIC IMPLEMENTATION IS EQUALLY IMPORTANT, AND ALL CRYPTOGRAPHIC PRODUCTS USED TO PROTECT NSS AND INFORMATION THEREIN MUST BE EVALUATED OR VALIDATED IN ACCORDANCE WITH CNSSP-11.

a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key

https://www.nsa.gov/ia/programs/suiteb_cryptography/

RFID Frequencies & Primary Use

121/3 Bar-Kochba St., Herzliya 46440 Israel 46440 הרצליה 121/3 בר כוכבא
+972.54.7504430 daniel@rfidgen.com

Low Frequency – profile

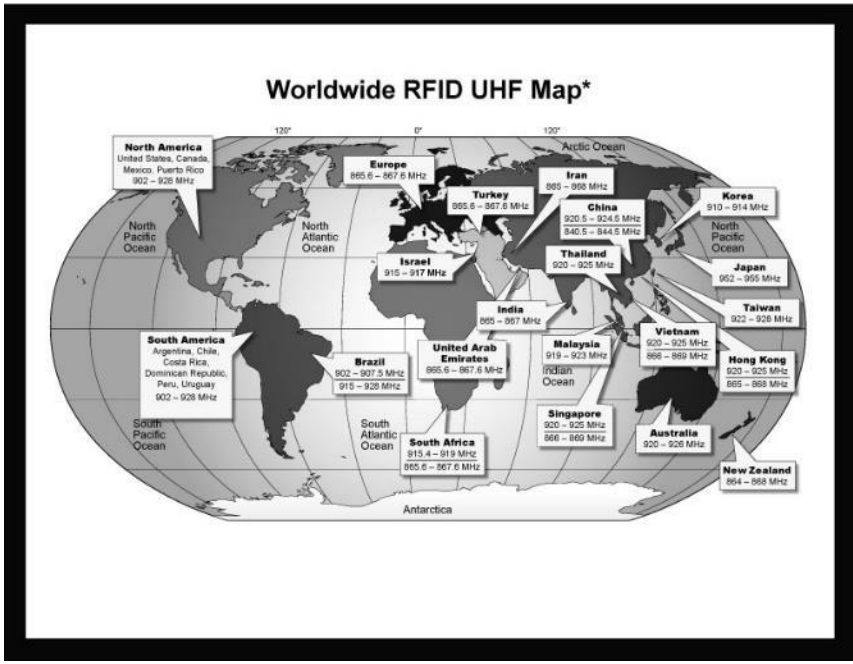
- **Frequency**: 125-134 KHz
- **Primary Uses**: Waste management, Animal Control (+ Automatic Fueling)
- **Security**: none or basic (PW protection)

- **Summary**: Suitable for harsh environment applications that require highly reliable, robust and safe data transmission. 10s of cm.

Ultra High Frequency – profile

- **Frequency**: 856 – 960 MHz. Specific in every country
- **Primary Uses**: Logistics
- **Security**: none or basic (PW protection)

- **Summary**: supply chain and logistics applications, high anti-collision rates, long read range (meters)



Gen ID Technologies Ltd

High Frequency – profile

- **Frequency**: 13.56MHz.
- **Primary Uses**: Payment, Identity, Authentication, nfc
- **Security**: High (Symmetric, Asymmetric, AES, 3DES, TK3DES, PW, ECC, ……)

- **Summary**: Technology used for most security related applications – credit cards, passports, authentication, access control, etc. Short range by design 2-15cm.

Active RFID– profile

- **Frequency**: mainly 433MHz and 2.4GHz.
- **Primary Uses**: RTLS, Continuous Monitoring.
- **Security**: Application Level Security.

- **Summary**: Relatively expensive “tags” provide continuous monitoring of tagged items. Long range, sensor additions.
  BLE is creating new market opportunities.

Security & Use Cases in RFID

Some examples from the over 4 Billion RFID tags currently deployed

121/3 Bar-Kochba St., Herzliya 46440 Israel 46440 הרצליה 121/3 בר כוכבא
+972.54.7504430 daniel@rfidgen.com

Many different RFID\NFC tags

- Over 50 different RFID ICs in common use
- RFID differ in:
  - Protocols
  - CPU or "Memory chip"
  - Security level
  - Multi-application
  - Memory size

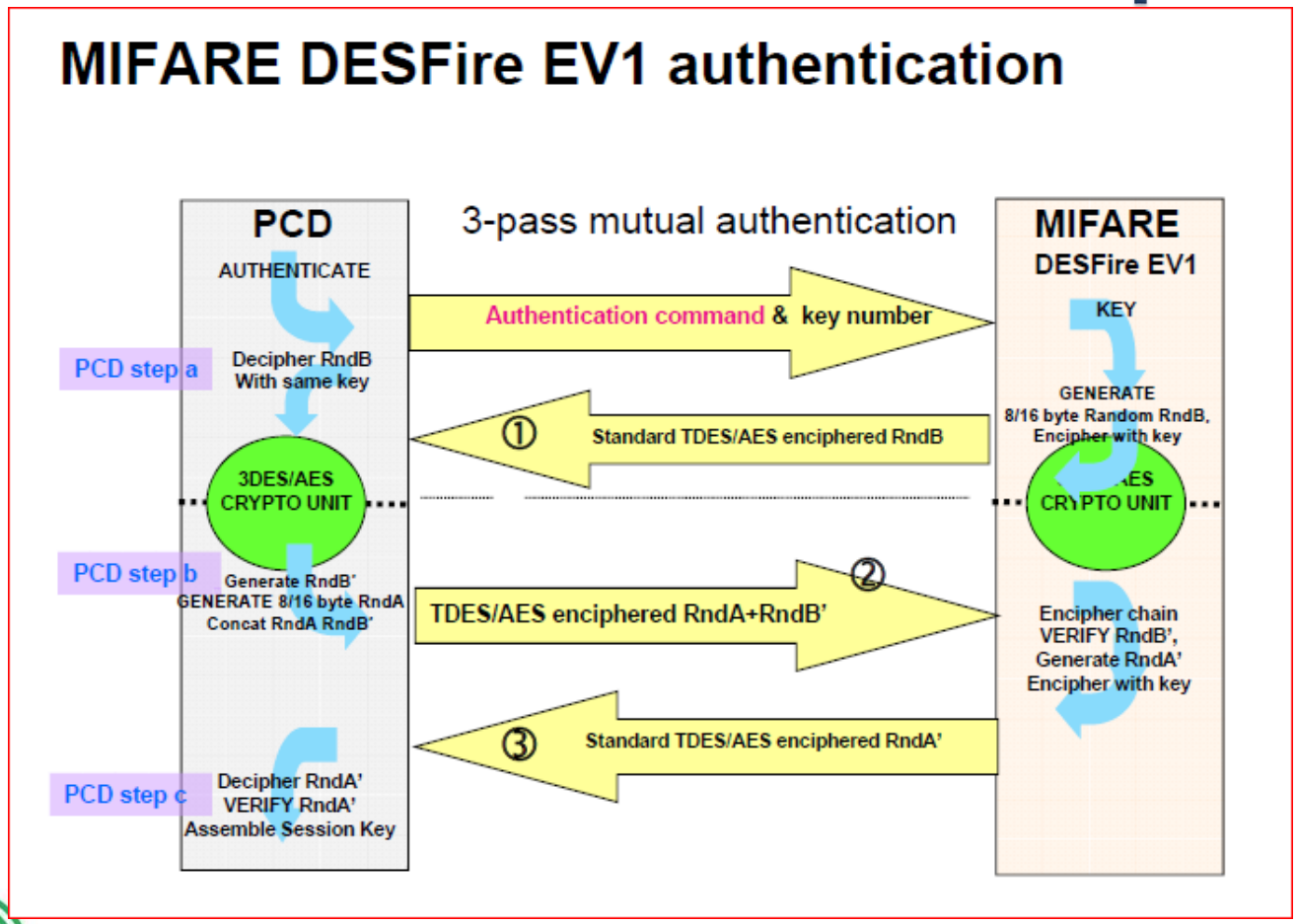
Feature	NTAG210	NTAG212	NTAG213	NTAG215	NTAG216
Usable Memory (Bytes)	48	128	144	504	888
32 bit Password	Yes	Yes	Yes	Yes	Yes
UID Ascii Mirror	Yes	Yes	Yes	Yes	Yes
24 bit Counter	-	-	Yes	Yes	Yes
Originality Signature	Yes	Yes	Yes	Yes	Yes
Fast Read Command	Yes	Yes	Yes	Yes	Yes
NFC Forum Type 2	Yes	Yes	Yes	Yes	Yes
7 Byte Unique ID	Yes	Yes	Yes	Yes	Yes

DESFire ® Platform Differences

	MF3IC40	MF3IC21–EV1	MF3IC41-EV1	MF3 IC D80
Memory Size	4k	2k	4k	**8k**
Internal Use				**256 bytes**
Free Space	4096 bytes	2272 bytes	4832 bytes	**7936 bytes**
Max. Applications	28	28	28	**28**
Max. Files per Application	16	32	32	**32**
Crypto	DES, TDES	DES, TDES	DES, TDES	**DES, TDES**
Life	10 Years	10 years	10 Years	**10 years**

rfidgen
Gen ID Technologies Ltd

Authentication – an example

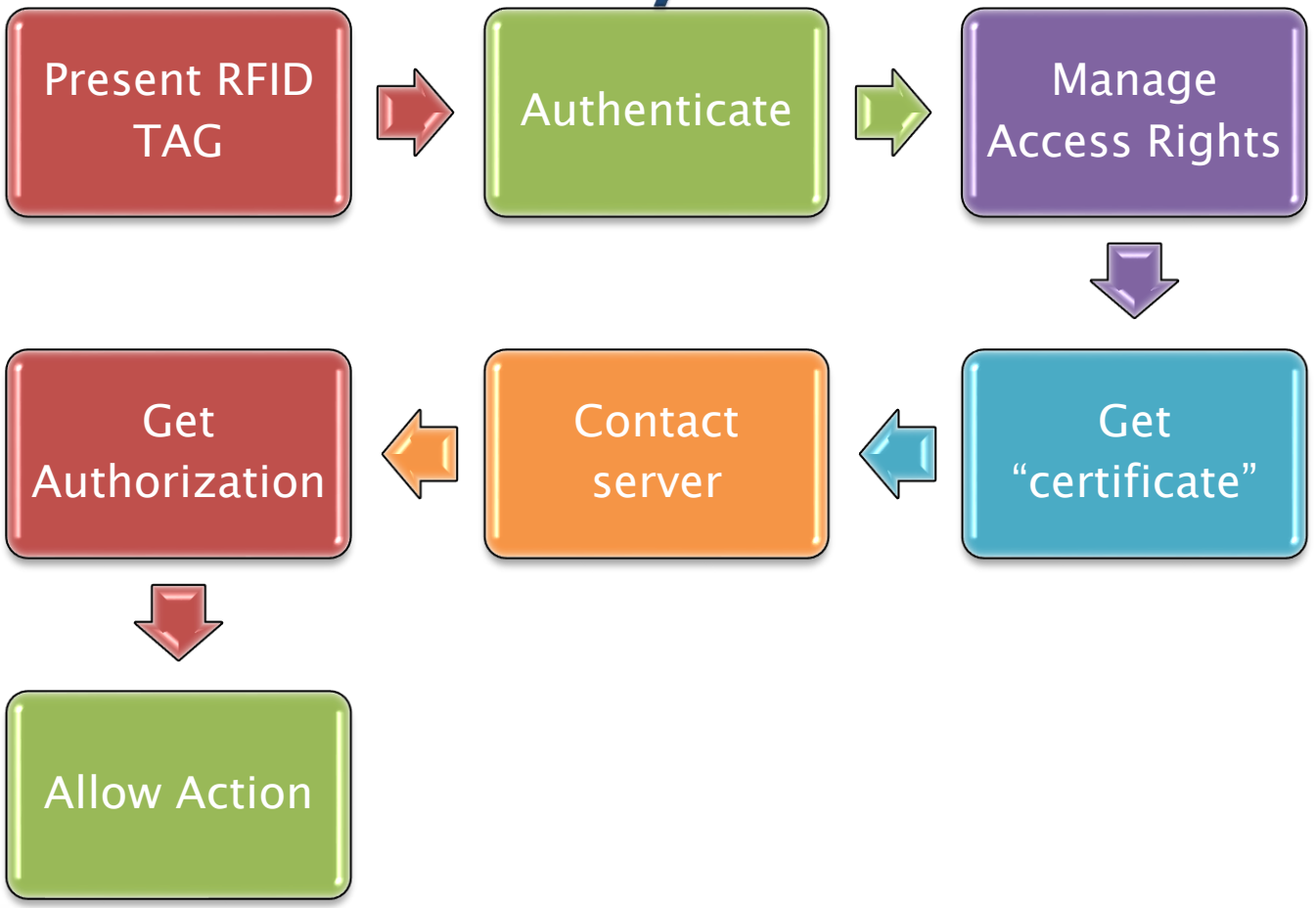


ID or Credential

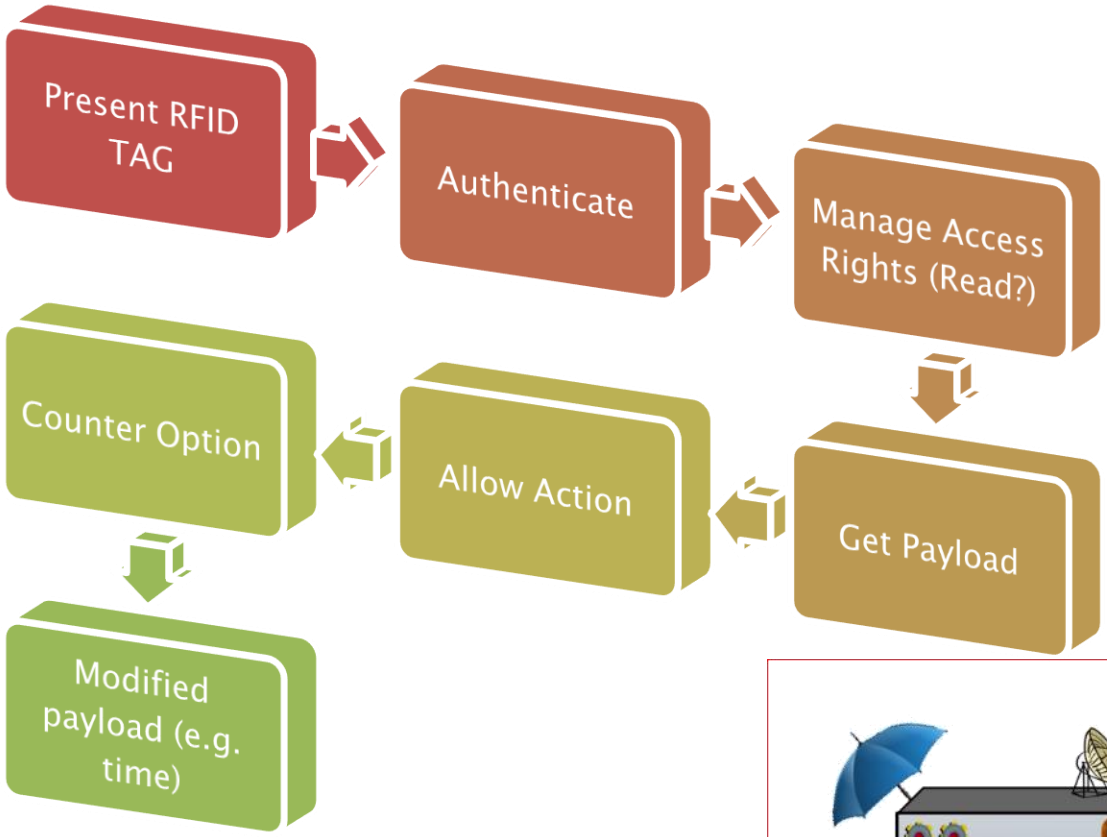
- Every tag has a UID.
- The UID may be used as part of the authentication process.
- Then you can enter the payload area.
- Payload may be encrypted at the application level.
- Your Credential should be protected in the payload area!

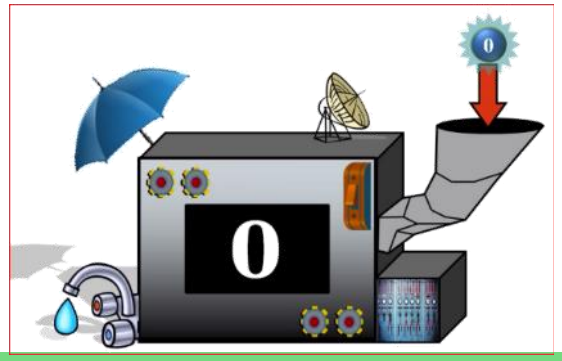
Gen ID Technologies Ltd

"on-line security"



"off-line security"





Gen ID Technologies Ltd

Access Control

- Today most Access Control in Israel is still based on Mag-stripe or low security RFID
- New projects are still based in UID (Unique-ID) of the rfid card. This can be emulated or cloned.
- Implementing a high security Access Control System is **NOT** necessarily more expensive.
- New technology is based on AES credentials or other secure mechanisms.

Gen ID Technologies Ltd

Passports

- Protected (for privacy) by an **open key** (MRZ)
- 144KBytes of information divided into different areas:
  - Public Area – MRZ
  - Private Areas – Private Keys

Gen ID Technologies Ltd

Credit Cards

- Paypass standard developed by Master Card.
- Other cards follow same or similar standards.
- Security must deal with cards, terminals, clearing systems, etc.

Cryptography & Security

- Encryption
  - PEK (PIN Encryption Key)
  - TPK (Terminal PIN Key)
  - TMK (Terminal Master Key)
  - Domain encryption
    - ZMK/ZCMK (Zone (Control) Master Key)
    - AWK (Acquirer Working Key)
    - IWK (Issuer Working Key)
  - Proprietary measures
    - MAC by terminal
    - Transport-level encryption

Public Transport

- Three main frameworks for managing security in the Public Transport market:
  - Old, hacked "***Mifare Classic***"
    - ***Proprietary crypto***
  - Calypso – Paris, Lisbon, Rio, Israel
    - Multi-Application platform
    - Cryptographic Operations performed in dedicated **SAMs**
  - Mifare DesFire EV1 – London, Madrid, Moscow
    - Multi-Application platform
    - Cryptographic Operations **may be** performed in dedicated **SAMs**

Public Transport Credentials and data may\should be protected in the payload area.

Consumables Protection

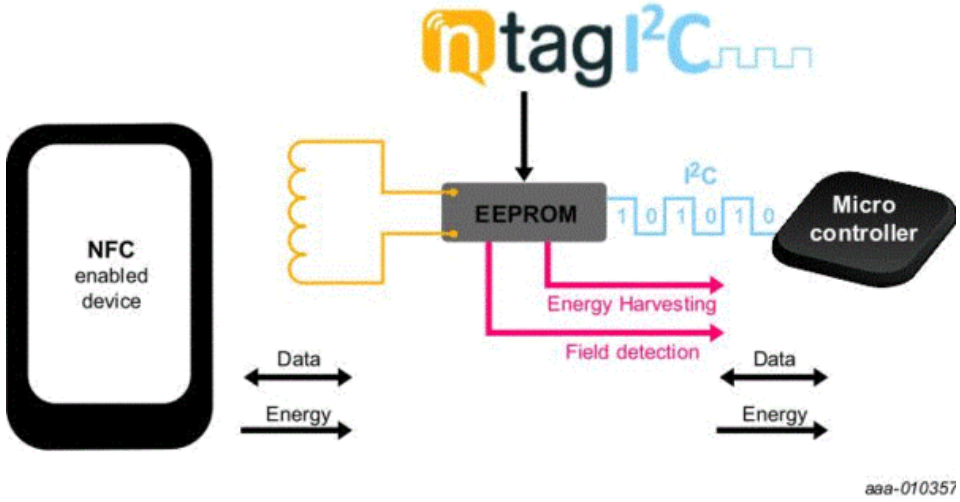
- Authentication is sometimes required in order to protect the business model.
- A specific credential can be designed based on existing, low cost rfid tags.
- A system approach is required in order to provide a cost effective solution (reader, tags, keys, production)

rfidgen
Gen ID Technologies Ltd

http://www.nxp.com/products/identification_and_security/smart_label_and_tag_ics/ntag/series/NT3H1101_NT3H1201.html

Tag with an Extension

- New tags have the option to connect to wired devices:
  - sensors (e.g. temperature)
  - Bridge to electronics
    - Configuration files
    - Log files
    - Authentication
    - Access



Clearing nfc Transactions

- Large ecosystem create a deployment "challenge"
- Some nfc tags provide the ability to encode all tags identically and provide different functionality: www.mytagfunction.com/**UID**
- Frameworks allow establishing functionality of the tag *IN THE CLOUD*
  - Examples:
    - Smart city
    - Coupons

Thank You

for more information please contact us:

Daniel Fainsod tel: +972 54 750.44.30
daniel@rfidgen.com

Gen ID Technologies Ltd