Intro to Cloud Encryption for Non-Techies

Concepts and Considerations

Alec Campbell
Excela Associates Inc.

IAPP Canada Symposium, May 2016

Introduction

- This is for a non-technical audience
  - Overview of concepts and issues
  - General discussion of advantages, disadvantages
  - Role of encryption in privacy protection for cloud-based data
  - Some policy implications

- For technical details, consult a security expert with cryptology expertise

What is encryption?

- Encoding information in such a way that only authorized parties can read it.
- Content is encrypted using an encryption algorithm, generating “ciphertext” that can only be read if decrypted.
- Theoretically possible to decrypt without the key, but not computationally feasible.
- Does not prevent interception - just denies the content to the interceptor.
- Password protection is NOT encryption.

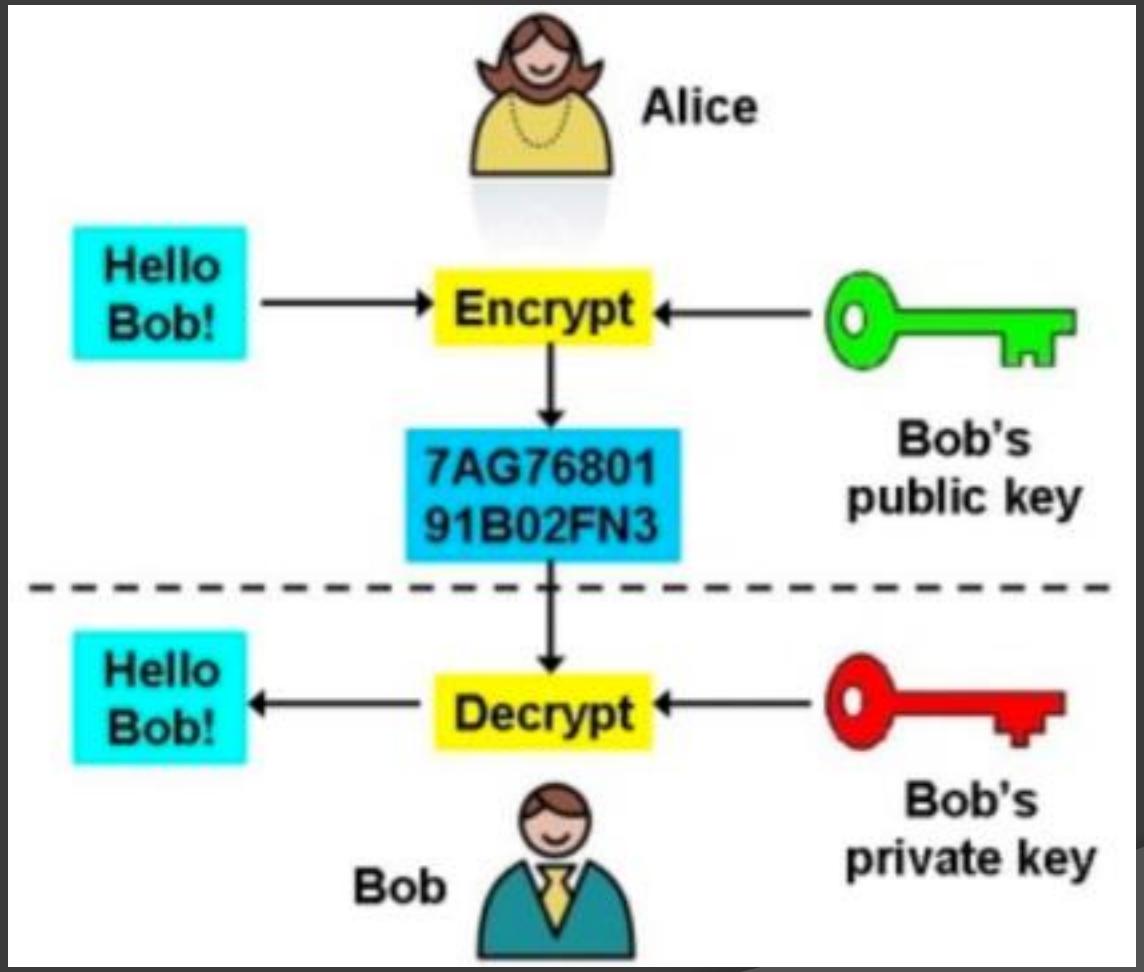
What is a “key”?

- Secret value used to encrypt or decrypt the data.
- Ensures only those with the key can read encrypted content.
- Your password is not the key, but may be used to generate the key.
- Keys are often also encrypted.

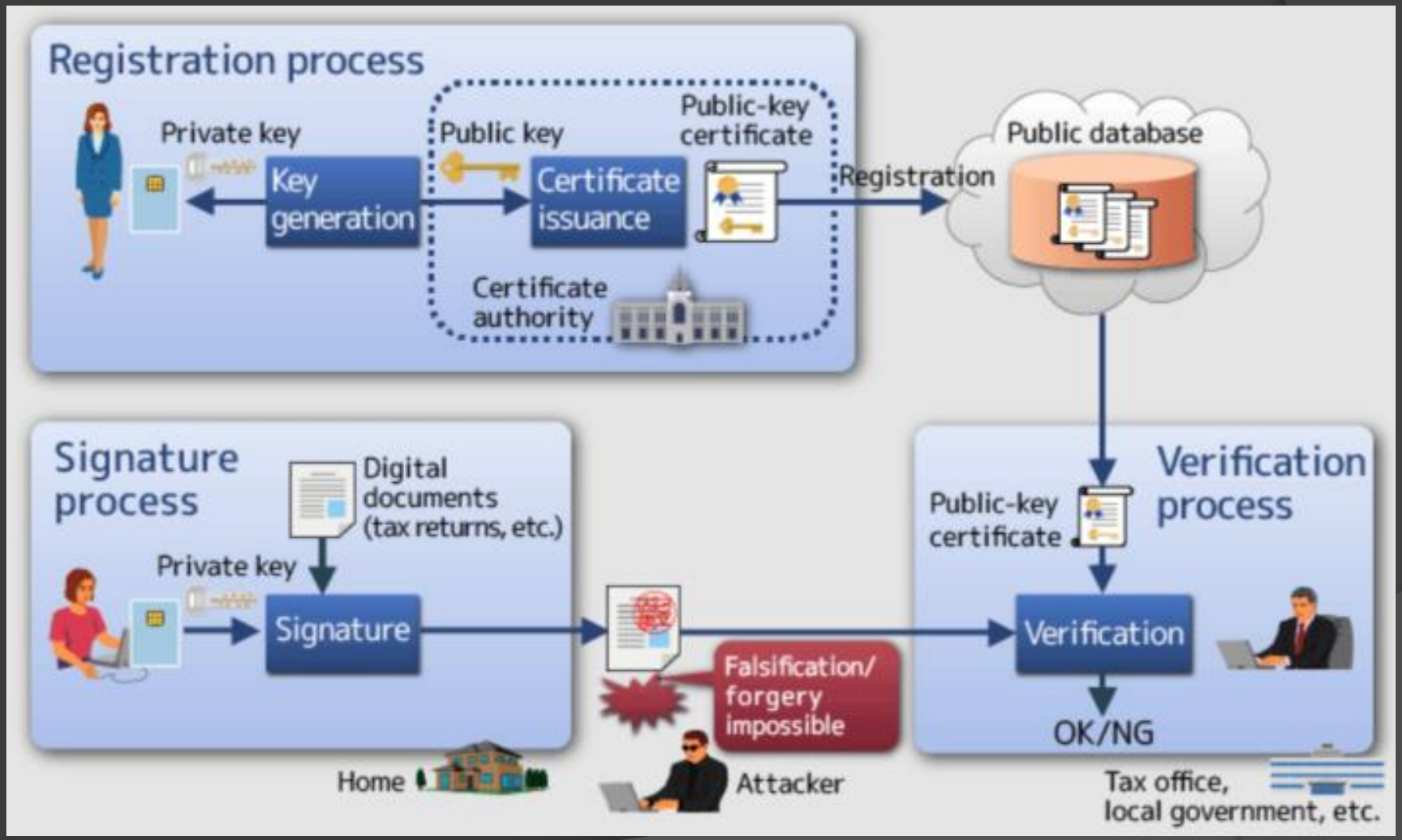
Encryption types

- Symmetric (e.g. AES, Twofish, etc.)
  - Use same key to encrypt and decrypt
  - Sender must provide key to receiver, often manually
- Asymmetric (PKI; e.g. PGP)
  - Private and public keys, usually exchanged automatically
  - Sender encrypts with receiver's public key (published)
  - Receiver decrypts with matching private key (secret)
- Special cases
  - SSL/TLS
  - Digital rights management (DRM)
  - Virtual private network (VPN)
  - Homomorphic encryption

Public Key Encryption



Public Key Infrastructure (PKI)



http://www.hitachi.com/rd/portal/contents/story/pbi/

How it's used

- Data in transit
  - Encrypted connection
    - Internet (SSL/TLS), wireless networks (WiFi, Bluetooth)
  - Encrypted communications data – e.g. encrypted e-mail attachment
- Data at rest
  - While stored on provider servers
  - While on workstation

Provider Encryption

- Most encrypt data in transit
  - SSL/TLS or via client-side encryption in app
- Some encrypt data on their servers
  - Most of these retain control of the keys
    - Protects from outside attacks
    - Does not protect against provider insider attacks
  - Some provide client control of keys
    - Protects against outsider and provider insider attacks
    - Does not protect against client insider attacks
    - Requires client key management

Zero Knowledge Encryption

- Term used when cloud provider cannot decrypt data
  - e.g., Apple/FBI debate
- Protects against attacks by outsiders and provider insiders
- Requires that client manage encryption keys
- May not be feasible if data need to be processed in the cloud
  - Future: homomorphic encryption

DIY Encryption

- Encrypt attachments to messages
  - manual or auto (using app)
  - desktop vs handheld
  - 3rd party products
- Encrypt data before transfer to cloud
  - software available
- Issues
  - Key management
  - Archiving and records management
  - Insider risks

Risks Addressed by Encryption

- Access by unauthorized persons or organizations
  - E.g., transmission errors, software bugs, device loss, etc.
  - Outsider snooping
  - Insider snooping (without keys)
- Reduces risk from outsider attacks
  - Hacking (without keys)
  - Theft of devices or storage media
- Improper disposal of personal info on electronic media
- Greatly reduces risks from accidental privacy breaches

Defeating encryption

- Insider attacks
  - Cannot protect against people with access to keys
  - Even zero-knowledge encryption is vulnerable to your own staff
- Obtain the key - “social engineering”
  - Phishing and other online exploits
    - E.g. email: “Your credit card account has been frozen…”
  - Key loggers
    - Requires physical access to device
- Brute force attack
  - Automated guessing of password
- “Back door”
  - E.g., proposals from some in law enforcement to have ‘secondary’ keys held in escrow
- Algorithmic flaws
  - Avoid proprietary encryption schemes – details of reputable schemes are public.

Management issues

- Loss or corruption of keys (key management)
- Difficulty processing data encrypted at rest
  - Future: homomorphic encryption
- Issues with long-term archival storage of encrypted data
- Painting a target
  - (It's encrypted so it must be important…)

- *All these issues can be managed.*

Legal Requirements

- Canadian legislation does not explicitly require encryption.
- But it does require adequate security measures to protect PI.
- For cloud services and portable devices, some level of encryption usually required for adequate protection,
  - E.g., HTTPS (SSL/TLS), whole-disk encryption
- Commissioners expect appropriate use of encryption.
- “Zero-knowledge” encryption is best, if you can manage its challenges.

Policy Issue Examples

- Privacy vs security
  - "Surveillance Society"
  - Law enforcement & national security
    - "back doors" – e.g. Apple/FBI, key escrow
- Contractual and legal issues
  - Whose laws apply? (hint: maybe not yours)
- Role and accountability of encryption service providers
  - Who is at fault for a breach?
  - Liability disclaimers
  - Cannot contract out of accountability

Summary

- Encryption greatly improves security of cloud-hosted data
  - Essential for data in transit
  - Highly desirable for data at rest
  - Zero-knowledge encryption best if feasible
- But encryption cannot protect against all risks
  - Provider insider attacks if provider holds keys
  - Client insider attacks when client holds keys
  - Social engineering (password theft)
- Use other methods for latter risks
  - Segregation of duties, internal key controls, training, etc.

Recommendations

- Cloud Security Alliance: sensitive data should be:
  - Encrypted for data privacy with approved algorithms and long, random keys;
  - Encrypted before it passes from the enterprise to the cloud provider;
  - Should remain encrypted in transit, at rest, and in use;
  - The cloud provider and its staff should never have access to decryption keys.
    - For processing decrypt to transient secure memory.

Resources - Information

- IAPP website
- Cloud Security Alliance
- Commissioners' websites

Resources – Software Examples*

- Encryption gateways
  - CipherCloud
  - Tresorit
- Encrypted storage, backup
  - iDrive (0K)
  - SpiderOak (0K)
  - MS OneDrive, Google Docs
- Encrypted email
  - Hushmail (Canada)
  - ProtonMail

** Excela does not endorse any product*

We're done!

Questions?

Alec Campbell

Excela Associates Inc.

780-945-0123

alec@excela.ca

www.excela.ca