SafeNet | THE DATA PROTECTION COMPANY

Digital Certificate

From 1024 to 2048

Kenny Lai

Information Security Consultant

Agenda

- Uses of Digital Certificates
- Importance of Key Length
- NIST's Recommendations
- Need for Advanced Cryptographic Technologies
- Global and Industry Trends
- Transition Plan of Recognized Certification Authorities (RCAs) in Hong Kong
- Experience Sharing for Implementation
- Queries in Your Mind
- Product Support Status
- General Checklist for Transition

SafeNet. THE DATA PROTECTION COMPANY

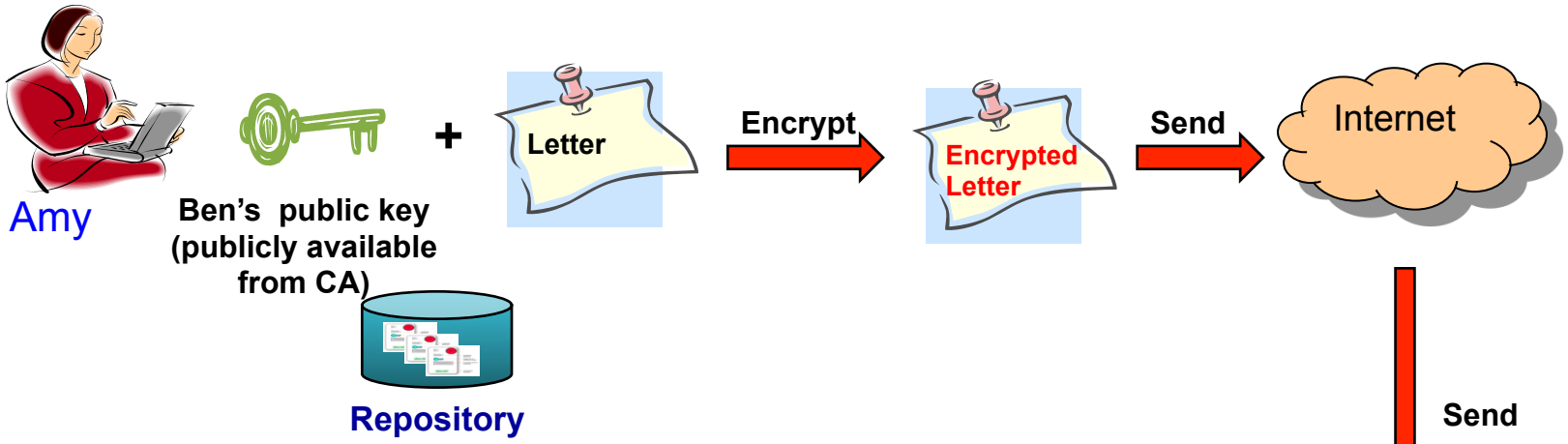
Uses of Digital Certificates

Digital certificate adopts the Public Key Infrastructure (PKI) framework for enabling the deployment of its three major functional uses –

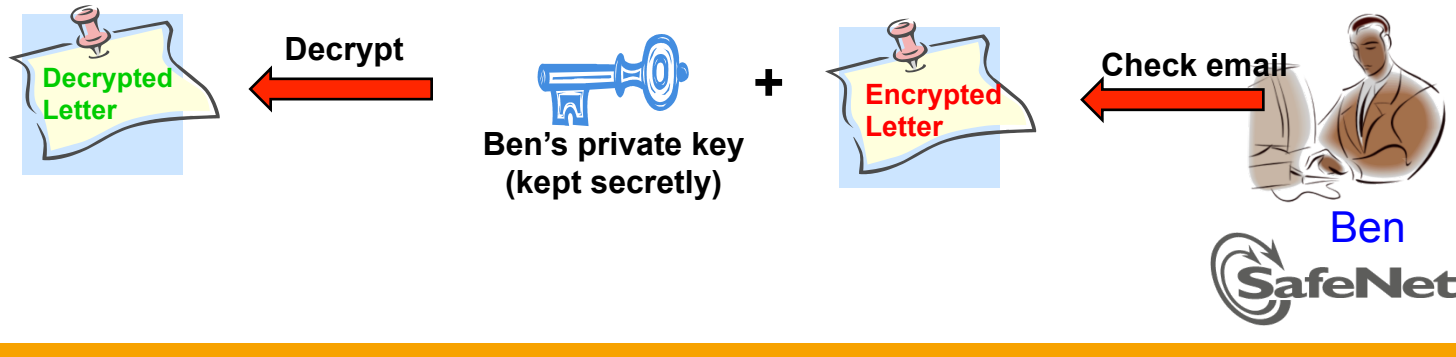
- Encryption / Decryption
- Digital Signature
- Electronic Authentication

Recap: Encryption / Decryption

1. **Amy uses Ben's public key to encrypt her letter and then sends it to Ben through email.**



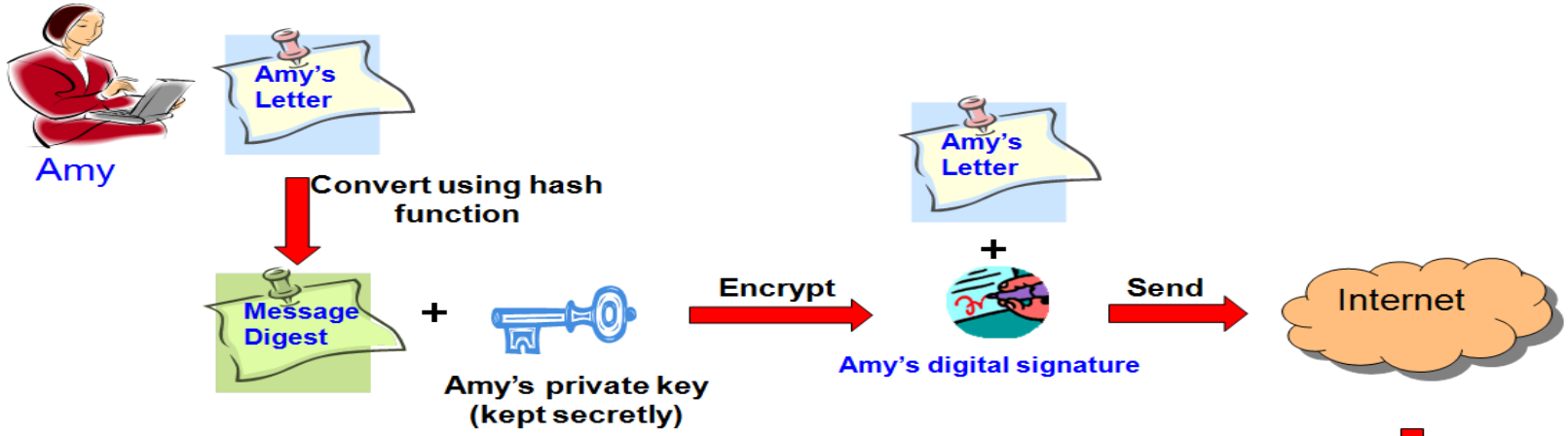
2. **Ben, upon receiving the email, decrypts Amy's email with his own private key.**



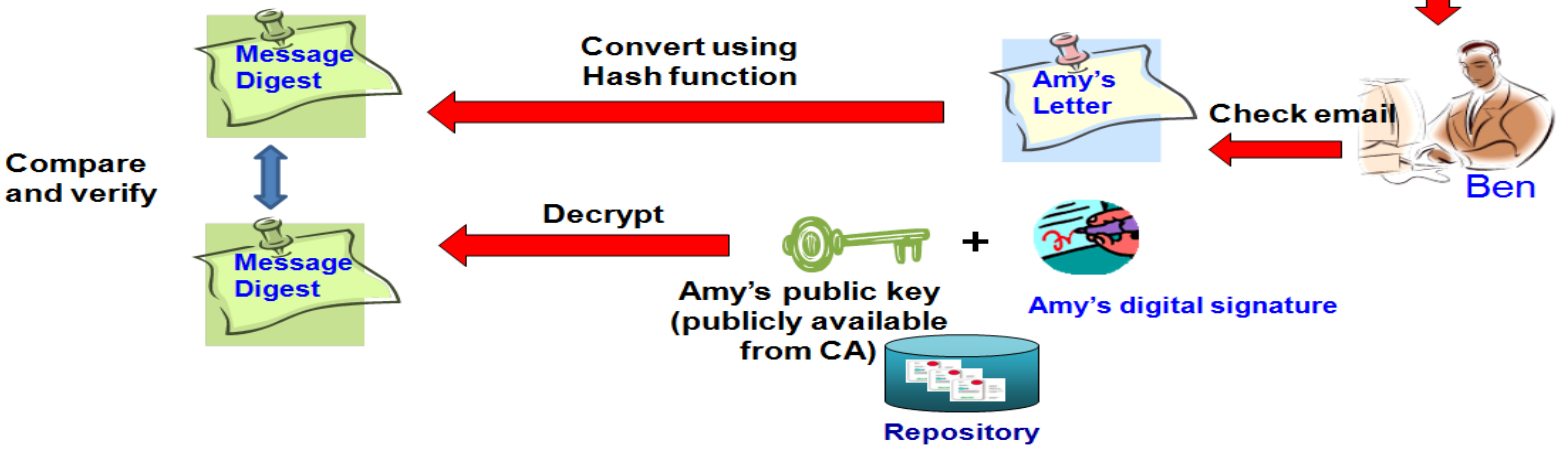
THE DATA PROTECTION COMPANY

Recap: Digital Signature

1. Amy converts her letter into a message digest by using a hash function. She then creates her digital signature by encrypting the message digest using her private key. Her letter, together with her digital signature are sent to Ben via email.



2. Ben, upon receiving the email, verifies Amy's digital signature using Amy's public key to decrypt the message digest by comparing the other one converted from the letter using the same hash function.



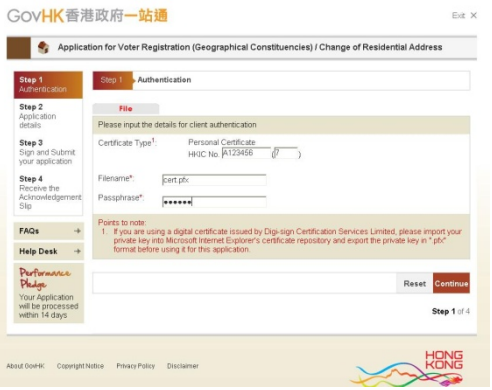
Recap: Electronic Authentication

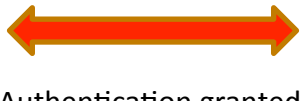
Smart ID Card embedded with digital certificate

Amy

\+

PIN





Authentication granted

Importance of Key Length

In cryptography, **key size** or **key length** is the size measured in bits of the key used in a cryptographic algorithm (e.g. RSA)

- longer key length  stronger security

However, the commonly used key size – **1024-bit** – is becoming not safe anymore……..

NIST's Recommendations

- National Institute of Standards and Technology (NIST) of the United States
  - published a guide SP800-131A in January 2011
    - recommending federal agencies to plan for transitioning to the use of longer cryptographic key lengths and more robust cryptographic algorithms
    - providing guidance on some areas of focus :
      - Signing with RSA algorithm should be transited from 1024-bit to 2048-bit by end of 2013
      - Hash function for digital signature generation should be transited from SHA-1 to SHA-2 by end of 2013
      - Use of Triple DES algorithm should be transited from 2 to 3 distinct keys by end of 2015

Need for Advanced Cryptographic Technologies

- Trend of adopting cryptographic technologies
  - to ensure the robustness of secure information exchange and electronic transactions
- Prevailing cryptographic algorithms and key length in use may not be sufficiently strong in projected future
  - key length and hash functions for digital signatures
  - encryption algorithms
- Trend of adopting stronger cryptographic methods and solutions for PKI
  - longer key length and stronger hash functions

Global Trends (1/5)

United States

NIST
National Institute of Standards and Technology

In January 2011, NIST recommended federal government agencies to :

- move to 2048-bit RSA keys and SHA-2, and
- stop using 1024-bit RSA keys and SHA-1 after 2013

FPKIPA
Federal Public Key Infrastructure Policy Authority

Personal Identity Verification (PIV) Cards

Commencing on 1 January 2011, CAs are required by federal government to use SHA-2 to generate digital signatures for signing PIV cards

Global Trends (2/5)

Department of Defense's (DoD) SHA-2 Transition Strategy

- Provide guidance with roadmap and milestones
- Engage vendors & manufacturers to determine plans for product support of SHA-256
- Upgrade systems & applications to handle SHA-256 as soon as possible but not later than 31 Dec 2012
- Infrastructure can begin to issue SHA-256 as soon as IT infrastructure can support its use but not later than 1 Jan 2013

Global Trends (3/5)

Mainland China

In March 2009, the China Internet Network Information Center (CNNIC), the state network information center of China, took the lead to increase **RSA key from 1024 bits to 2048 bits** for :

- Root Certificates
- Intermediate Root Certificates
- SSL Certificates

Global Trends (4/5)

Taiwan

GCA 政府憑證管理中心

XCA 組織及團體憑證管理中心

- In Aug 2009, Government Certification Authority (GCA) and miXed Organisation Authority (XCA) start issuing 2048-bit 憑證 IC Card
- 1024-bit 憑證 IC Card can be used until expiry of validity period

- Commencing from 1 Jan 2011, Healthcare Certification Authority (HCA) starts issuing Healthcare Identity Card (HCA 2.0) with 2048-bit certificates (10 years validity period)

Global Trends (5/5)

Estonia

Estonia's Electronic ID Cards are carrying 2048-bit certificates for encryption and digital signatures

Usages :

- i-Voting,
- Apply for universities
- Update automobile registry
- File tax return
- Health Insurance
- Access medical records; e-prescriptions
- Internet banking

Industry Trends (1/2)

- Mozilla will disable or remove all root certificates with RSA key sizes smaller than 2048 bits from the trust list by end 2013.
- Network Security Services support SHA-2.

Microsoft

- Microsoft announced its Microsoft Root Certificate Program required all new root certificates to have a 2048-bit RSA key as minimum.
- Microsoft will no longer accept root certificates with 1024-bit RSA of any expiration.
- Windows products support SHA-2, with appropriate patches and updates.

Industry Trends (2/2)

- Apple's OS X and iOS have already supported 2048-bit key.

- Red Hat recommends to use 2048-bit RSA in its Certificate System Deployment Guide.
- Red Hat Enterprise Linux 5.6 supports SHA-2 algorithms in Domain Name Service Security Extensions (DNSSEC).

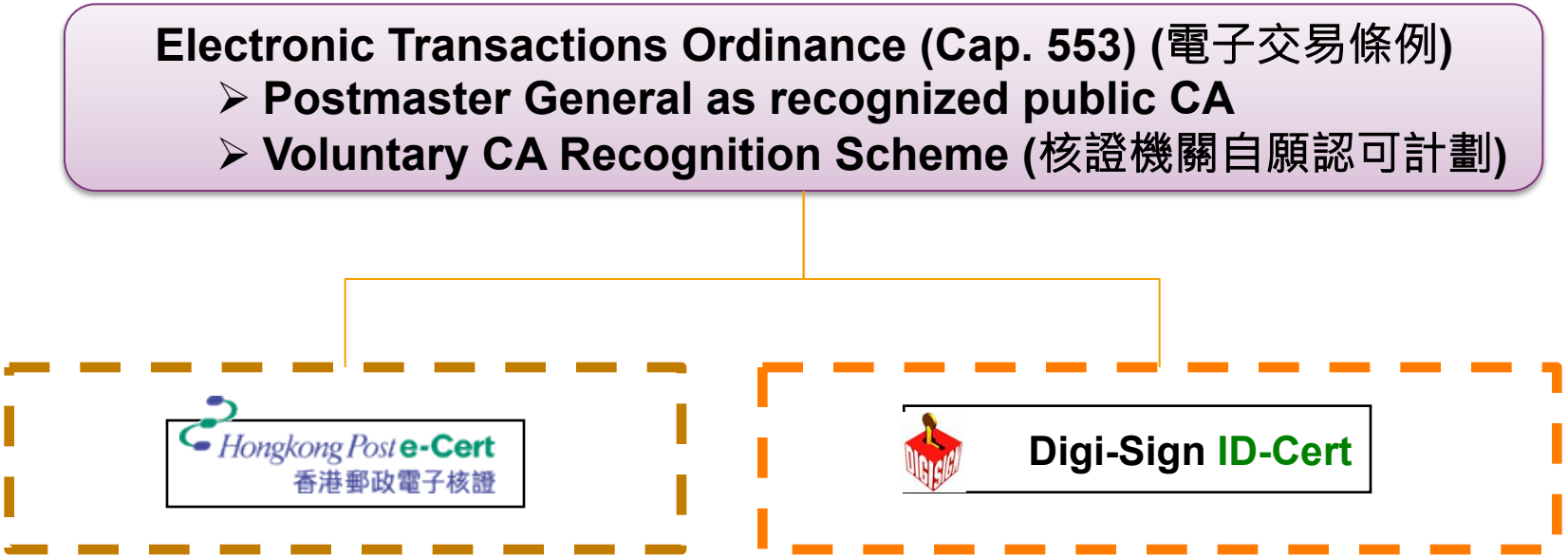
- Supports 2048-bit RSA digital signing.
- Can use 3rd party digital ID, or creating one using Acrobat.

Major Certification Authorities (CAs)

- Major overseas CAs have already migrated from 1024-bit to 2048-bit RSA keys
- Most of their certificates are also SHA-2 ready

SafeNet. THE DATA PROTECTION COMPANY

Transition Plan of the Two RCAs in Hong Kong



- Hongkong Post Certification Authority (HKPCA)
- Digi-Sign Certification Services Limited (Digi-Sign)

HKPost CA Transition Plan (1/2)

		1024-bit e-Cert	2048-bit e-Cert
e-Cert (Personal) e-Cert (Organisational) e-Cert (Encipherment)	From 28 Jun 2012 – 31 Dec 2013	Default	On-Request
	From 1 Jan 2014 onwards	Retired	Default

- Applicants who wish to apply for e-Cert with 2048-bit RSA key length should assess or consult their respective service providers on whether the intended systems or software can support the use of e-Cert with 2048-bit RSA key length.

HKPost CA Transition Plan (2/2)

		1024-bit e-Cert	2048-bit e-Cert
e-Cert (Server)*	From 1 Dec 2011 – 30 Nov 2012	1-year-validity	2-year-validity
	From 1 Dec 2012 onwards	Retired	Default

* e-Cert (Server) is the only Recognized SSL certificate in HKSAR.

- Applicants who wish to apply for e-Cert with 2048-bit RSA key length should assess or consult their respective service providers on whether the intended systems or software can support the use of e-Cert with 2048-bit RSA key length.

SafeNet. THE DATA PROTECTION COMPANY

Transition Plan of Digi-Sign

	1024-bit ID-Cert	2048-bit ID-Cert
From 1 January 2012 to 31 December 2013	Default	On Request
From 1 January 2014 onwards	Ceased	Default

- For the avoidance of doubt, subscribers can continue to use their existing 1024-bit ID-Certs until their natural expiry
- Subscribers who wish to use 2048-bit ID-Certs are advised to contact their respective relying parties to confirm the readiness of their systems or applications on the support of 2048-bit certificates

SafeNet. THE DATA PROTECTION COMPANY

Who Should Care

CA

- Certificate Issue

Company

- Web Server Support
- Application Readiness
- Performance Impact

End User

- Browser Support
- PKI Token Support

SafeNet. THE DATA PROTECTION COMPANY

Performance Impact to Existing SSL Enabled Applications

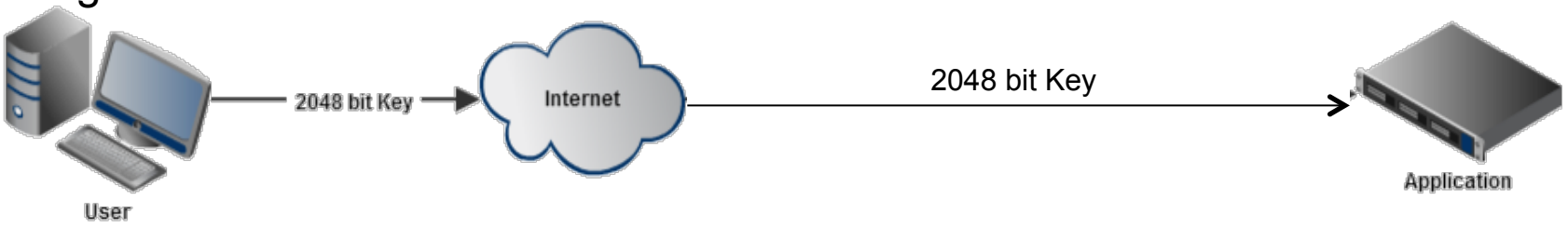
- On average 80% TPS drop
- Only 1/5 transactions can be handled if switched to 2048-bit key
- Hardware upgrade to compensate the loss in performance
- Dedicated hardware for key storage to compliant to regulation

SafeNet. THE DATA PROTECTION COMPANY

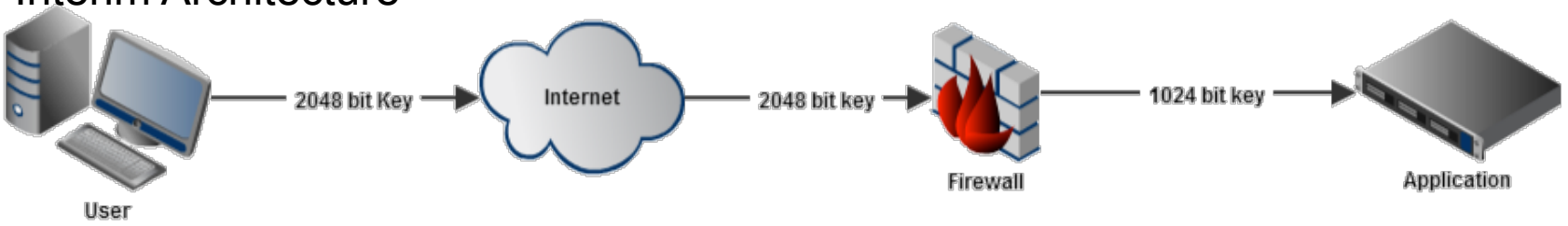
Legacy Web System Handling

- Use firewall which has capability to decrypt 2048-bit key and re-encrypt with 1024-bit key
- Legacy system can still communicate with external when upgrade of application is not yet possible
- Weaker security

Target Architecture



Interim Architecture



SafeNet. THE DATA PROTECTION COMPANY

Speed Up Document Signing Capability with HSM

- Token is design for personal use with limited processing power
- For batch document signing, certificate generation, HSM can be used
- Capable to handle 2048 to 4096bits certificate
- Extreme performance boost compare with Token processing power
- Same or higher level of security (FIPS Level 3)

SafeNet. THE DATA PROTECTION COMPANY

Queries in Your Mind (1/6)

Q. What are the risks if the transition cannot be completed by the stated deadline?

A. Applicants may no longer be able to subscribe for 1024-bit Recognized Digital Certificates once they are retired. Applicants are recommended to assess or consult their respective service providers on whether the intended systems or software can support the use of digital certificates with 2048-bit RSA key length before respective CA ceases issuing the intended 1024-bit digital certificates.

SafeNet. THE DATA PROTECTION COMPANY

Queries in Your Mind (2/6)

Q. Will there be any interoperability issues during the transition period from existing cryptographic technologies to the advanced ones?

A. There may be interoperability issues during transition. Applications need to “Bilingual” – capable to handle both old and advanced crypto technologies.

Queries in Your Mind (3/6)

Q. When the new 2048-bit recognized digital certificates issued by recognized certification authorities (RCAs) becomes available, should users subscribe the new ones and revoke the existing one before its natural expiry?

A. Normally, there would be a transition period when both key lengths can co-exist. Users need not immediately revoke existing digital certificates and may renew them at the time of expiry. Before acquiring new 2048-bit digital certificates, users should ensure the applications in use can support new 2048-bit digital certificates and perform necessary testing before deployment.

Queries in Your Mind (4/6)

Q. How should the legacy data (those digitally signed or encrypted with the existing algorithms and key) be handled during and after the adoption?

A. Depends on the data category, if the data is archive, we suggest keeping its original form and keep the old key in case decryption or signature verification is required.

For active data, to simplify the management effort, suggest rekeying with new key.

SafeNet. THE DATA PROTECTION COMPANY

Queries in Your Mind (5/6)

Q. Does HK Smart-ID Card support 2048-bit Digital Certificate?

A. Smart-ID Card is in the progress of moving from 1024-bit to 2048-bit Digital Certificate. Meanwhile, Hongkong Post provides e-Cert File (USB) and USB-Token that both support 2048-bit Digital Certificate.

SafeNet. THE DATA PROTECTION COMPANY

Queries in Your Mind (6/6)

Q. Why SHA-256 is chosen for upgrade instead of other block sizes among the SHA-2 family (224/384/512)?

A. SHA-256 is chosen for upgrade mainly because of wide support of 32-bit words systems (SHA-256 uses 32-bit words while SHA-512 uses 64-bit words, SHA-224 & SHA-384 are the truncated versions of SHA-256 & SHA-512 respectively).

SafeNet. THE DATA PROTECTION COMPANY

Product Support Status

1. Browser / OS Platforms
2. Browser / Mobile OS Platforms
3. Mail Clients (S/MIME)
4. Hardware Tokens
5. Web Servers
6. Application Servers
7. PDF

SafeNet. THE DATA PROTECTION COMPANY

Browser/OS Platforms

Browser	Operation System	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
Internet Explorer 6-8	Microsoft Windows XP	Microsoft	Y	Y	2048-bit RSA: Windows XP SP3 SHA-256: Windows XP SP3 + fix pack
Internet Explorer 7 or above	Windows Vista	Microsoft	Y	Y	
Internet Explorer 8 or above	Microsoft Windows 7	Microsoft	Y	Y	
Safari 4 or above	Mac OS X 10.6 or above	Apple	Y	Y	
Safari 4 or 5	Microsoft Windows XP, Vista and 7	Microsoft	Y	Y	Safari supports Windows 7 starting from version 4.0.3
Konqueror	Red Hat Enterprise Linux (RHEL)	Red Hat	Y	Y	It requires RHEL 5.x to support 2048-bit RSA and SHA-256 RHEL 5.6 supports SHA-2 algorithms in Domain Name Service Security Extensions (DNSSEC).
Mozilla Firefox 3.5 or above	Microsoft Windows XP, Vista and 7	Microsoft	Y	Y	
	Mac OS X 10.6 or above	Apple	Y	Y	
	Red Hat Enterprise Linux (RHEL)	Red Hat	Y	Y	It requires RHEL 5.x to support 2048-bit RSA and SHA-256
Google Chrome	Windows, Mac OS and Linux	Google	Y	Y	

SafeNet. THE DATA PROTECTION COMPANY

Browser/Mobile OS Platforms

Browser	Operation System	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
Safari 4-5	iOS 4	Apple	Y	Y	iOS 4.0 use OCSP for certificate revocation checking
Safari 4-5	iOS 5	Apple	Y	Y	iOS 5.0 use OCSP for certificate revocation checking
Default "Browser"	Android	N/A	Y	Y	2048-bit RSA: Android 2.3 or above
IE mobile	Microsoft Windows Phone 7	Microsoft	Y	Y	It has no UI to view the certificate

SafeNet. THE DATA PROTECTION COMPANY

Mail Clients (S/MIME)

Product	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
IBM Lotus Notes	IBM	Y	N	Lotus Notes ver 7.0 or above for 2048-bit RSA key. It has no SHA-256 roadmap.
BlackBerry (S/MIME Support Package)	CSL	Y	Y	S/MIME Support Package Version 4.5 or later for BlackBerry devices with BlackBerry Enterprise Server Version 4.1 SP 5 or later
Microsoft Outlook	Microsoft	Y	Y	Outlook 2007 or 2010 running on Windows Vista or 7

SafeNet. THE DATA PROTECTION COMPANY

Hardware Tokens

Product	Support 2048-bit RSA	Support SHA-256	Remarks
eToken	Y	Y	• eToken 5100/5200 with Hardware version 8.0 or above and Firmware version 1.0 or above
eToken PRO	Y	N SHA-1 only	• eToken PRO can support SHA-1 only • eToken PRO 32K/64K/72K with Hardware version 4.29 or above and Firmware version 1.0 or above • eToken PRO 32K/64K with CardOS 4.2B and above • eToken PRO 72K with Java based OS 4.28 and above
eToken PRO Anywhere	Y	N SHA-1 only	• eToken PRO Anywhere can support SHA-1 only • eToken PRO Anywhere with Hardware version 4.33 or above and Firmware version 4.0.7 or above
iKey	Y	N SHA-1 only	• iKey 4000/2032 can support SHA-1 only • iKey 2032 with Hardware version 0.6 and Firmware version 2.0.

SafeNet. THE DATA PROTECTION COMPANY

Web Servers

Product	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
Microsoft IIS	Microsoft	Y	Y	2048-bit RSA: IIS 5.0 on Windows 2000 or above SHA-256: IIS 7.5 on Windows Server 2008
IBM Websphere HTTP Server	IBM	Y	Y	2048-bit RSA: version 6.1 SHA-256: version 7 + GSKit 7.0.4.14 or above
IBM Websphere Application Server	IBM	Y	N	2048-bit RSA: version 6.1 + fix pack SHA-256: will be supported in future product fix packs
Oracle Weblogic Server	Oracle	Y	Y	2048-bit RSA: Weblogic 10.3.x SHA-256: Weblogic 12C
Apache based Server	N/A	Y	Y	SHA-256: Apache version 2.x or higher with Open SSL 1.1.x

SafeNet. THE DATA PROTECTION COMPANY

Application Servers

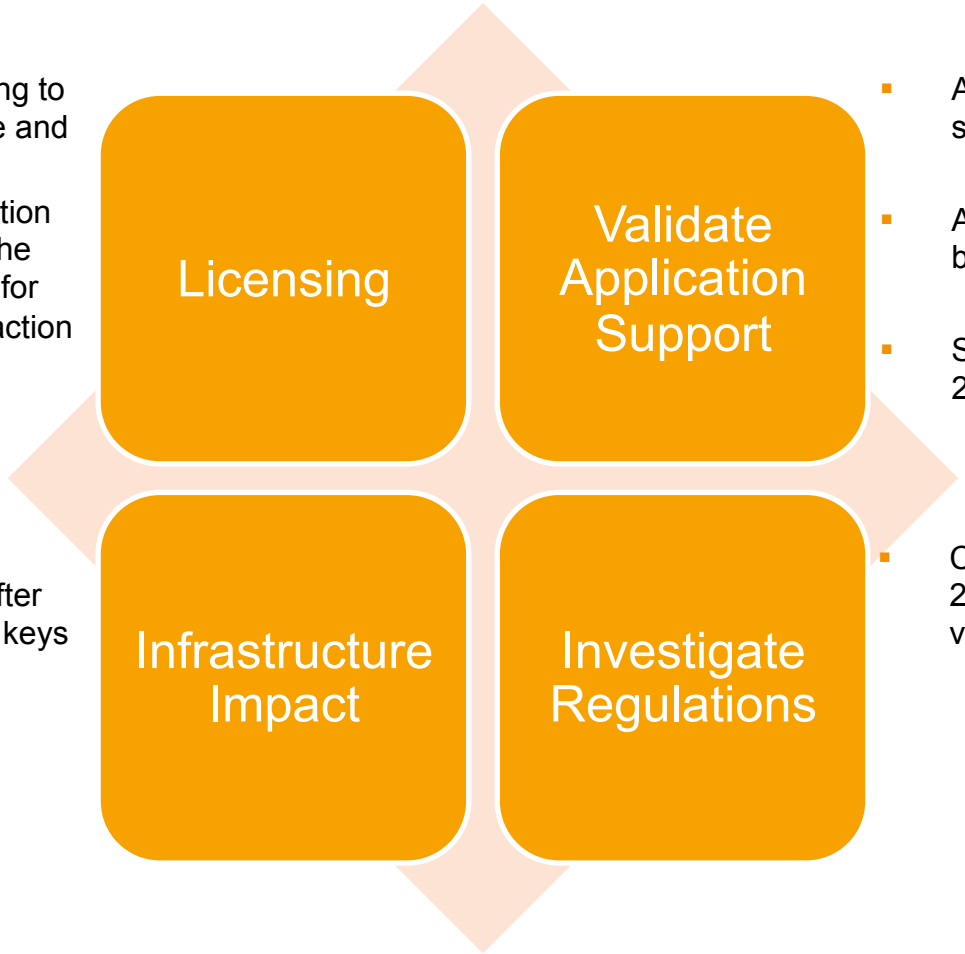
Product	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
Oracle Identity Federation (OIF)	Oracle	Y	Y	2048-bit RSA: OIF 11g SHA-256: Requires Weblogic 12C
Novell Access Manager	Novell	Y	Y	2048-bit RSA: version 3.0 SHA-256: version 3.0
CA SiteMinder	CA	Y	Y	Required SiteMinder and Federation R12.0 to perform SiteMinder R12 SP3 infrastructure to support 2048-bit RSA key & SHA-256
Microsoft Sharepoint	Microsoft	Y	Y	2048-bit RSA: Windows 2000 or above SHA-256: Windows Server 2008
Jboss Application Server	Red Hat	Y	Y	2048-bit RSA: JDK 1.5+ /Jboss EAP 4+ SHA-256: JDK 1.5+ /Jboss EAP 4+
IBM Tivoli Federated Identity Manager	IBM	Y	Y	2048-bit RSA: version 6.2.2 SHA-256: version 6.2.2
IBM Lotus Domino	IBM	Y	N	2048-bit RSA: Lotus Notes 7.0 or above
IBM Websphere Portal	IBM	Y	N	2048-bit RSA: version 6.1 + PM20116 SHA-256: Will be supported in future product fix packs
Java based Server	N/A	Y	Y	SHA-2: Java SDK 1.4.2 or higher is installed on the server.

PDF

Product	Vendor	Support 2048-bit RSA	Support SHA-256	Remarks
Adobe Reader and Acrobat	Adobe	Y	Y	2048-bit RSA: PDF 1.5 (Acrobat 6.0) SHA-256: PDF 1.6 (Acrobat 7.0)

General Checklist for Transition

- Software/Hardware Licensing to support the required feature and throughput
- Divide existing SSL transaction count by five to determine the new required license count for enabled 2048bit SSL transaction



- Adding incoming 2048-bit key support
- Ability to detect incoming key bits
- Switch from 1024-bit key to 2048-bit key

- Evaluate the performance impact to existing system after adding support for 2048-bit keys

- Check regulation for storing 2048-bit certificate/keys in FIPS validated container

SafeNet. THE DATA PROTECTION COMPANY

Thank You!

SafeNet. THE DATA PROTECTION COMPANY