



AC
ML



The Era of Electronic Test Report and Digital Signature 電子測試報告及數碼簽署時代

Association of Construction Materials Laboratories Ltd.

Ir. Stanley Chan

Content:

1. Environmental Issue with Testing laboratories
2. Digital Test Report in Hong Kong
3. Digital Signature
4. Hongkong Post e-Cert
5. Validation of Documents
6. Points to note

1. Environment Issue with Testing Laboratory

Global Warming

2023年全国平均气温创历史新高

国家气候中心 2024-01-03 11:13 北京



你想知道的气候信息都在这里!

[点击上方关注我们](#)

2023年，全国平均气温 10.7°C ，较常年 (9.9°C) 偏高 0.8°C ，为1961年以来最高，打破2021年 10.5°C 记录。全国大部地区气温偏高 $0.5\sim 1^{\circ}\text{C}$ 。山东、辽宁、新疆、贵州、云南、天津、湖南、河北、四川、河南、北京、内蒙古、广西等13个省（市、区）气温均为1961年以来历史最高，全国共127个国家气象站日最高气温突破历史极值。

September 7, 2023




South China Morning Post Latest China Economy HK Asia Business Tech Lifestyle People & Culture World Comment Video Sport Post Mag Style - AI

and midnight on Thursday.

Listen

The black rainstorm alert was issued on Thursday night, the first since October 2021.

The torrential rain, which continued into Friday morning, also forced the closure of border control points at Heung Yuen Wai and Man Kam To, as well as services at city immigration offices, all public clinics and postal operations.



Floodwater conquered roads and even malls overnight in Hong Kong. Photo: Edmond So

The image shows a large, multi-level indoor mall or public space that has been severely flooded. The ground floor is completely submerged in murky, brown floodwater. Debris, including what appears to be a chair and some papers, is scattered in the water. On an upper level, a group of people is standing behind a glass railing, looking down at the flooded area. The architecture features large white pillars and a modern design.

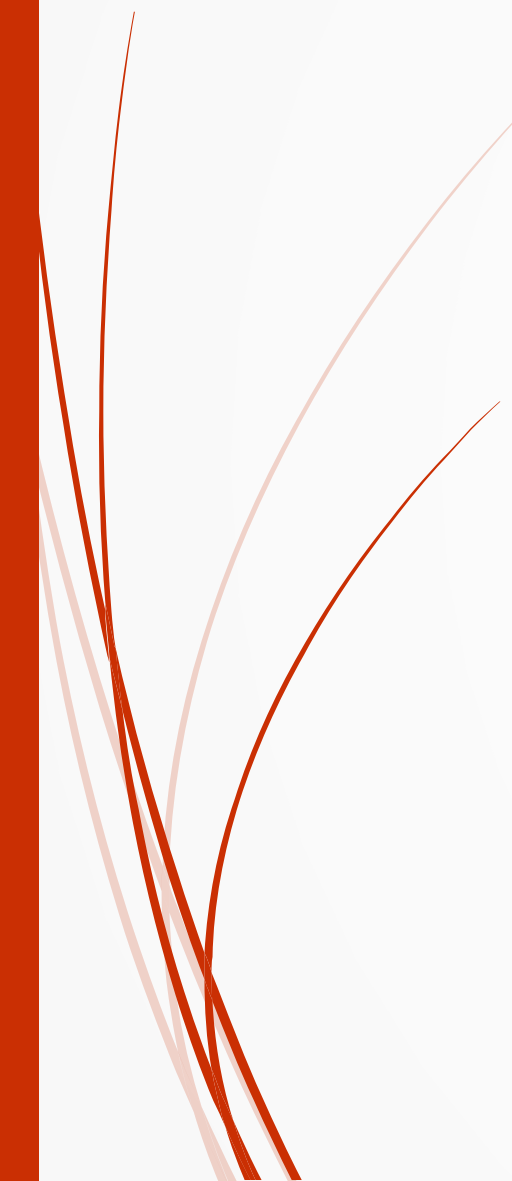
- <https://www.scmp.com/news/hong-kong/health-environment/article/3233782/hong-kong-observatory-issues-red-rainstorm-alert-warns-significant-road-flooding>



China's Goal to Carbon Emission

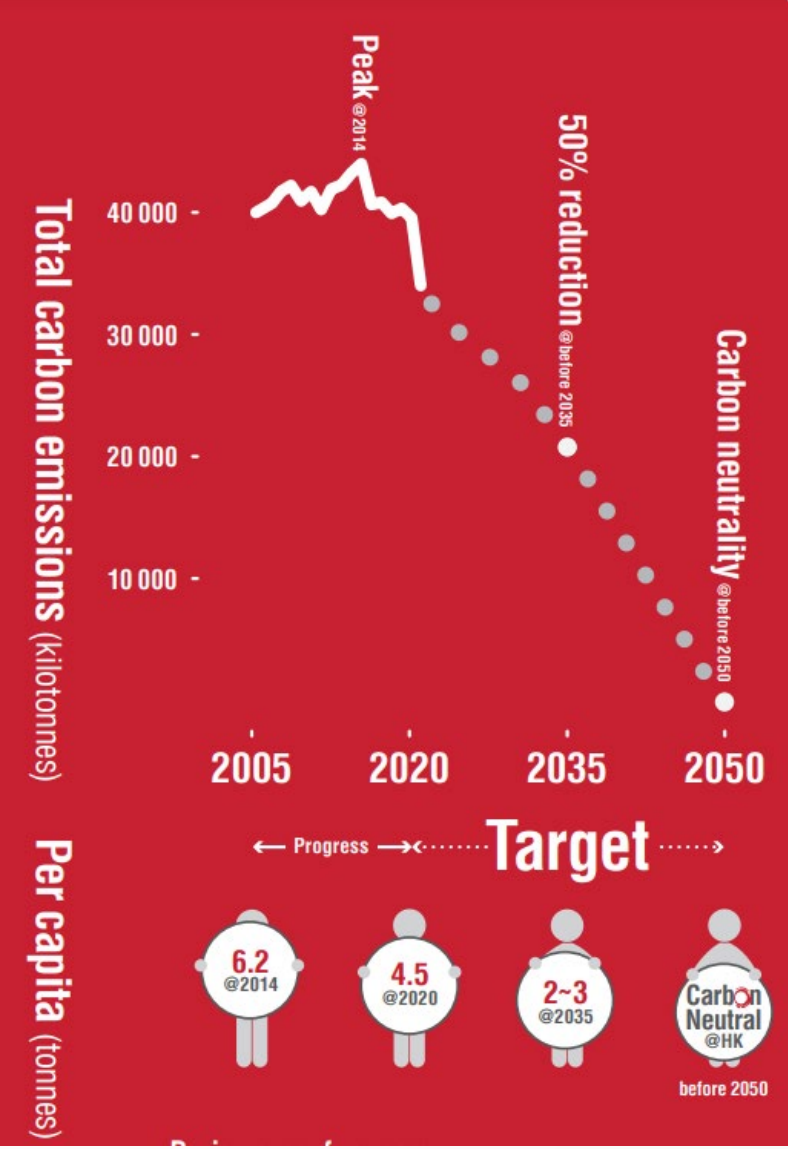
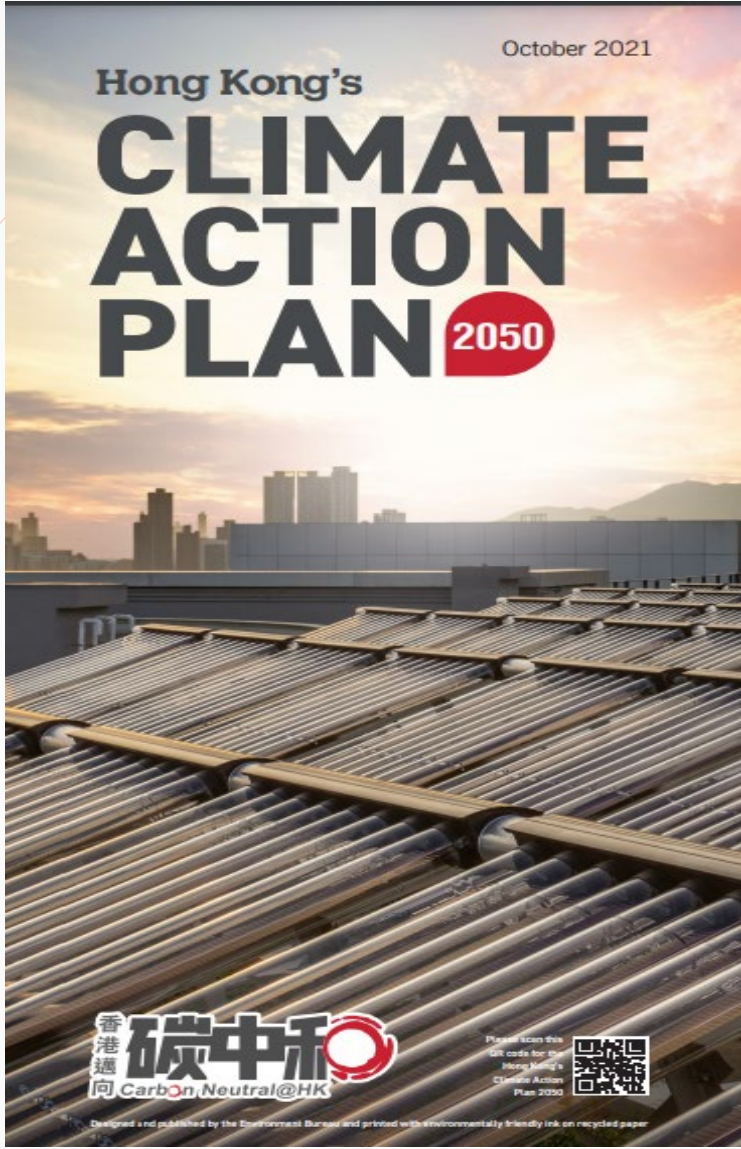


AC
ML

- 
- ▶ Achieve its peak of carbon emission before 2030
 - ▶ Achieve carbon neutrality before 2060

Hong Kong's Commitment

- ▶ Achieve carbon neutrality before 2050
- ▶ Reduce by 50% before 2035 as compared to the 2005 level



Can we do something?

- Reduction of paper usage because paper has a large carbon footprint
- Paper consumption is huge in our testing industry
- All the hardcopy test reports are the final product to our client



Paper Carbon Footprint

Life Cycle of Paper product:

- ▶ Source – Tree are cut
- ▶ Production process – energy and chemical use during processing
- ▶ Transportation – shipping of paper
- ▶ Use – From raw paper to usable paper product
- ▶ Disposal – Methane gas generation at landfill

A decorative graphic on the left side of the slide features a vertical orange bar, a horizontal orange arrow pointing right, and several thin, curved lines in shades of orange and red that sweep across the page.

2. Digital Report in Hong Kong

Electronic Test Report Hong Kong

- ▶ Hong Kong Housing Authority, Started on Jan 1, 2023

C7 Reporting of Test Results

The Laboratory shall submit 1 original of test reports to the Senior Project Officer. When instructed by the Contract Manager, the Laboratory shall submit test reports in digital format with digital signature. Test report shall be dispatched according to the time schedule specified in Part D of this Specification for each type of test. For tests with no reporting time schedule specified, reporting shall be within 7 days from the completion of the respective test items. 1 more day will be given if photographs (3R) are to be included in the reports. The period indicated above shall exclude Saturday, General Holidays and days during which the Tropical Cyclone Warning Signal No. 3, or higher, or the Black Rainstorm Warning, is in force.

Electronic Test Report Hong Kong

- ▶ CEDD, Started on August 1, 2023

Submission of Test Reports

In accordance with Clause 22 of the Specification, please be instructed that the issue of **electronic test reports with digital signature** shall take effect on **1 August 2023**. The reports shall be submitted to the project offices and copied to the PWL by e-mail with details as presented in the aforesaid Clause.

HOKLAS SC-33



HOKLAS SC-33
Issue No. 10
Issue Date: 28 July 2023
Implementation Date: 28 July 2023
Page 10 of 13

5.6 A HOKLAS endorsed report or certificate shall be signed by a HOKLAS approved signatory of the issuing laboratory. For printed reports or certificates, such signature shall be made in hand-written form. For reports or certificates in an electronic form, the electronic signature shall be in a form acceptable under the Electronic Transactions Ordinance (Cap. 553). The full name of the approved signatory (as in his/her identity document such as identity card or passport) shall be clearly shown alongside the signature.



A digital certificate can be carried in Hong Kong Identity Card, installed in your personal computers / notebooks and other storage devices such as USB flash drive, etc. and it is usually protected by a personal identification number (PIN) of the person's own and the person will be asked to enter the PIN in using the digital certificate for electronic transactions.

Under the [Electronic Transactions Ordinance \(Cap. 553\)](#) (ETO), digital signature generated by digital certificate has the **same legal status as paper-based signature** and can satisfy the signature requirement under the law when transacting with the Government. For transactions not involving the Government, any form of electronic signature including digital signature also has the same legal recognition and can meet the signature requirement under the law so long as it is reliable, appropriate and agreed by the recipient.

Cap 553

Electronic Transaction Ordinance

AC
ML

(1) Where—

- (a) a rule of law requires the signature of a person (*the first mentioned person*) on a document or provides for certain consequences if the document is not signed by the first mentioned person; and
- (b) neither the first mentioned person nor the person to whom the signature is to be given (*the second mentioned person*) is or is acting on behalf of a government entity,
an electronic signature of the first mentioned person satisfies the requirement if—
- (c) the first mentioned person uses a method to attach the electronic signature to or logically associate the electronic signature with an electronic record for the purpose of identifying himself and indicating his authentication or approval of the information contained in the document in the form of the electronic record;
- (d) having regard to all the relevant circumstances, the method used is reliable, and is appropriate, for the purpose for which the information contained in the document is communicated; and
- (e) the second mentioned person consents to the use of the method by the first mentioned person. (*Replaced 14 of 2004 s. 5*)

6. 電子簽署、數碼簽署等

(1) 凡——

- (a) 任何法律規則規定須由任何人(前者)在某文件簽署，或規定該文件未由前者簽署則會有某些後果；及
- (b) 前者及將會提供該簽署的人(後者)均既非政府單位亦非代表任何政府單位行事

則在以下情況下，前者的電子簽署即屬符合該規定——

- (c) 前者使用某方法使該電子簽署與某電子紀錄相連或在邏輯上相聯，以識別自己和顯示自己認證或承認包含於以該電子紀錄形式存在的該文件內的資訊；
- (d) 就傳達包含於該文件內的資訊的目的而言，在顧及所有有關情況下，所使用的該方法是可靠和適當的；及
- (e) 後者同意前者使用該方法。(由2004年第14號第5條代替)

Cap 553

Electronic Transaction Ordinance

AC
ML

(1A) Where—

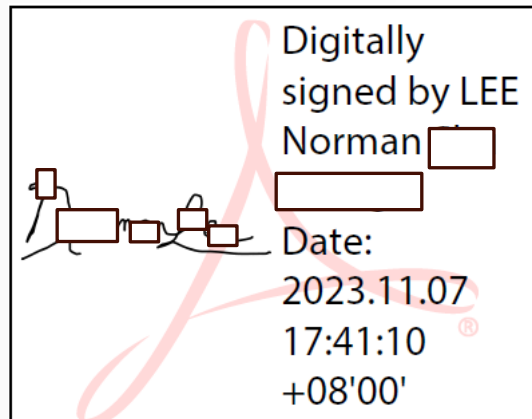
- (a) a rule of law requires the signature of a person on a document or provides for certain consequences if the document is not signed by the person; and
 - (b) either or both of the person mentioned in paragraph (a) and the person to whom the signature is to be given is or are or is or are acting on behalf of a government entity or government entities,
- a digital signature of the person mentioned in paragraph (a) satisfies the requirement if the digital signature is—
- (c) supported by a recognized certificate;
 - (d) generated within the validity of that certificate; and
 - (e) used in accordance with the terms of that certificate.

(Added 14 of 2004 s. 5)

(1A) 凡——

- (a) 任何法律規則規定須由任何人在某文件簽署，或規定該文件未由該人簽署則會有某些後果；及
 - (b) (a)段所述的人及將會獲提供該簽署的人(或其中一人)是政府單位或代表某政府單位行事，
- 則在以下情況下，(a)段所述的人的數碼簽署即屬符合該規定——
- (c) 有認可證書證明該數碼簽署；
 - (d) 該數碼簽署是在該證書的有效期內產生的；及
 - (e) 該數碼簽署按照該證書的條款使用。(由2004年第14號第5條增補)

3. Digital Signature? Electronic Signature?



Electronic Signature vs Digital Signature



Digital Signature	Electronic Signature
Authorized and Regulated by Certification Authority	Not authorized
High security – documents and signature are encrypted	Lower security
Can be verified	Cannot be verified
A slightly more complicated authentication process	Fast, Simple and Easy to use
For document with sensitive information such as transaction	Good for documents that does not contain sensitive information
Require a certified digital ID and PIN	Various method to verify signer identity such as email, PIN

HKHA Contract Requirement



C33 Security Requirements on IT/Data Communication Systems (Cont'd)

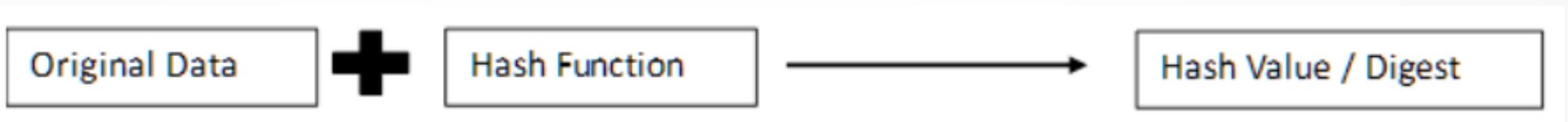
C33.3 Application Security Requirements (Cont'd)

- (viii) If XML is used, it shall not include sensitive data in XML document in clear-text. Extensible Stylesheet Language (“XSL”) can be used to transfer the XML document to exclude/encrypt sensitive information prior to delivery.
- (z) The system shall avoid on disclosing system information through the error handling process.
- (aa) The system shall have the central module developed to record all audit trails, exceptions and generate error logs.
- (bb) If digital signature is implemented, digital signature suites with 2048-bit RSA key and SHA-256 shall be used.

SHA 256

AC
ML

- **Secure Hash Algorithm**, hash value 256 bits
- One-Way Process – Irreversible
- Hash function provides same output value if input is unchanged
- Main purpose: Check if data is modified



RSA 2048

- Asymmetric cryptosystem, i.e. Two-Way (Public + Private Key)
- Both side does not have the same secret key
- Encryption method
- Use to “Digitally- sign” the report

Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

ong Post Root CA 2
ngkong Post e-Cert CA 2 - 15

Summary Details Revocation Trust Policies Legal Notice

Certificate data:

Name	Value
RFC822 email	
Certificate policies	<see details>
Public key	RSA (2048 bits)
SHA1 digest of p...	<see details>
X.509 data	30 82 06 3A 30 82 05 22 A0 03 02 01 02 ...
SHA1 digest	E3 2D CC DF 7D CE 56 32 CE C0 24 05 E...
MD5 digest	72 3E 47 A1 93 FE A8 10 8D C3 E0 CD 19...

《電子交易條例》
(第 553 章)

Electronic Transactions Ordinance
(Cap. 553)

AC
ML

verify a digital signature (核實數碼簽署), in relation to a given digital signature, electronic record and public key, means to determine that—

- (a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and
- (b) the electronic record has not been altered since its digital signature was generated,

and any reference to a digital signature being verifiable is to be construed accordingly.

- (2) For the purposes of this Ordinance, a digital signature is taken to be supported by a certificate if the digital signature is verifiable with reference to the public key listed in a certificate the subscriber of which is the signer.

(Amended 14 of 2004 s. 2; L.N. 131 of 2004)

證書 (certificate) 指符合以下所有說明的紀錄——

- (a) 由核證機關為證明數碼簽署的目的而發出，並且該數碼簽署的用意是確認持有某特定配對密碼匙的人的身分或其他主要特徵的；
- (b) 識別發出紀錄的核證機關；
- (c) 指名或識別獲發給紀錄的人；
- (d) 包含該獲發給紀錄的人的公開密碼匙；並且
- (e) 由發出紀錄的核證機關簽署；(由 2004 年第 14 號第 2 條修訂)

- (2) 為施行本條例，如某數碼簽署可參照列於某證書內的公開密碼匙得以核實，而該證書的登記人是簽署人，則該數碼簽署視作獲該證書證明。

(由 2004 年第 14 號第 2 條修訂；由 2004 年第 131 號法律公告修訂；編輯修訂——2017 年第 3 號編輯修訂紀錄)

A decorative graphic on the left side of the slide, featuring a vertical orange bar, a horizontal orange arrow pointing right, and several thin, curved lines in shades of orange and red that sweep upwards and to the right.

4. Hongkong Post e-Cert

How do I get it?

AC
ML



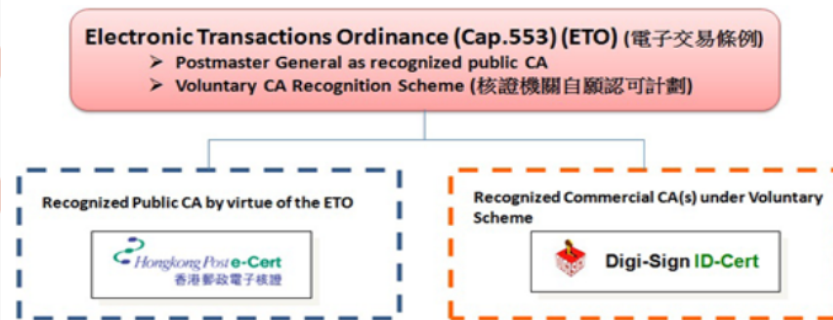
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

[About Us](#) [Our Work](#) [What's New](#) [Service Desk](#) [Contact Us](#) 繁體 Text Size

Recognized Certification Authorities in Hong Kong

Certification authorities (CAs) play an important role on the effective operation of the public key infrastructure (PKI) and as a credible third party to proof of identity of the parties involved in an electronic transaction.

Currently, there are two recognized CAs under the [Electronic Transactions Ordinance \(Cap. 553\)](#) (ETO) in Hong Kong. The Postmaster General is a recognized CA by virtue of the ETO and offers Hongkong Post Certification Authority services, whereas the Digi-Sign Certification Services Limited is a commercial recognized CA which has been granted recognition under the Voluntary CA Recognition Scheme of the ETO.



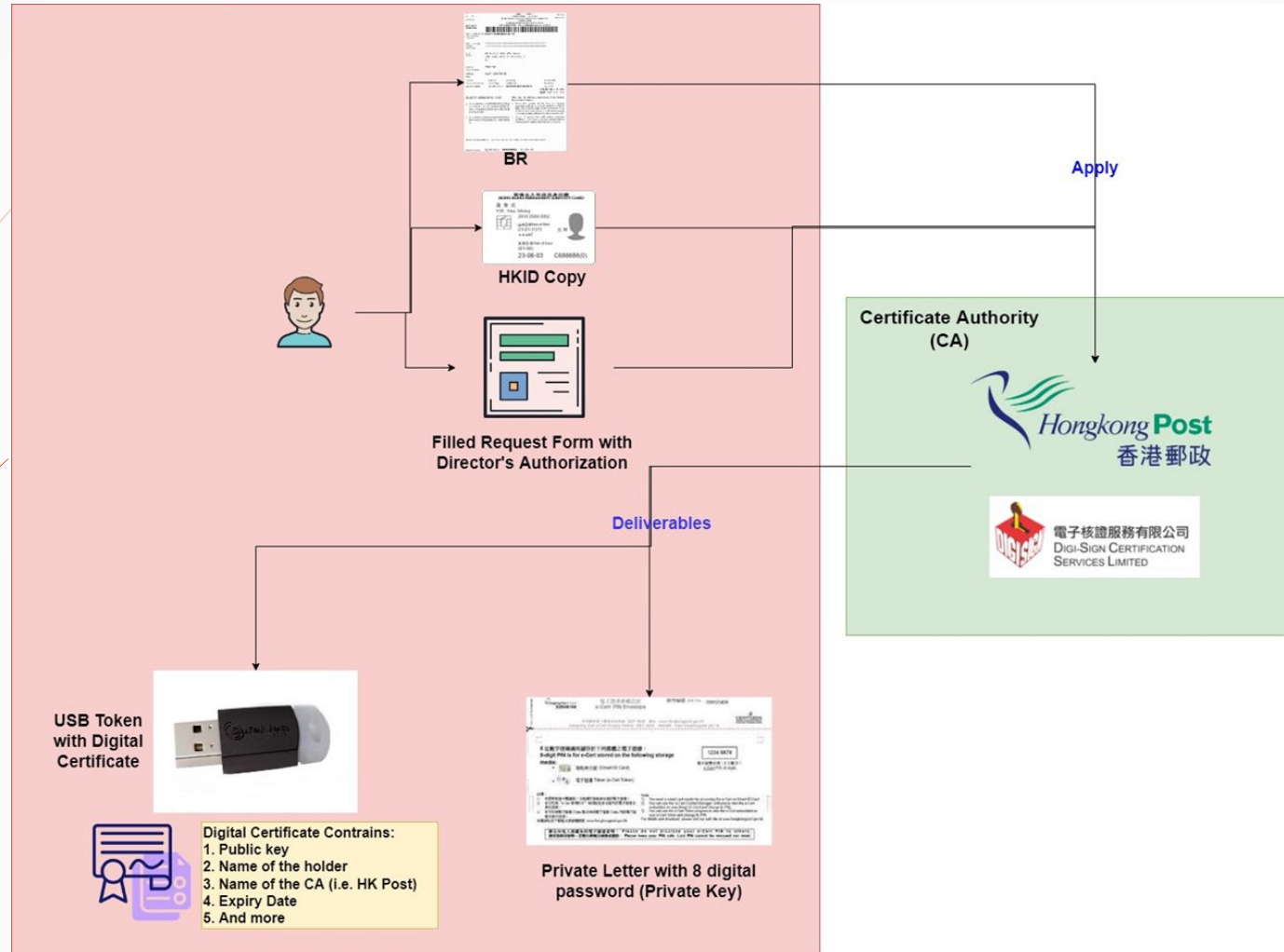
Hongkong Post e-Cert (Organisational) with “Mutual Recognition” Status Certificate



- Company apply/renew for their employee with **authorization** of “**director or a person with equivalent rank**”, **HKID, BR**
- Hongkong Post e-Cert as **Certificate Authority (CA)**
- A Hongkong Post e-Cert contains a **public key**, the name of the holder, an expiration date, a certificate serial number and subscriber reference number.
- **e-Cert Token** with **password** (SafeNet)
- Mutual Recognition means **trusted by Adobe®** for signing PDF documents(in term of **Adobe Approved Trust List, AATL**) → **Blue Ribbon** when open pdf with Adobe Reader
- Renew every **1/2/3 years**, hongkong post provide a **new token** with a **new certificate**



Application Procedure



List of AATL




FR	France	Vialink		
FR	France	Worldline		
HK	Hong Kong SAR of China	Digi-Sign		
HK	Hong Kong SAR of China	Hongkong Post		
ID	Indonesia	Vida		
IL	Israel	ComSign		
				

► <https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html>

Self-Signed Certificate

AC
ML

 Adobe Community

 Search this community

Trust a signer's certificate

Digital signatures that were added using a self-signed certificate cannot be automatically validated by Adobe as the certificate is not in the list of Trusted Identities that Adobe uses to validate signatures. A self-signed certificate is a certificate that you have generated yourself using a third-party application. You will not be able to manually validate the signature until the certificate is trusted by Adobe. If you open such a PDF, you will see a warning **At least one signature has problems.**



At least one signature has problems.

<https://community.adobe.com/t5/acrobat-discussions/validating-a-digital-signature/m-p/11934718#:~:text=A%20self%2Dsigned%20certificate%20is,least%20one%20signature%20has%20problems.>

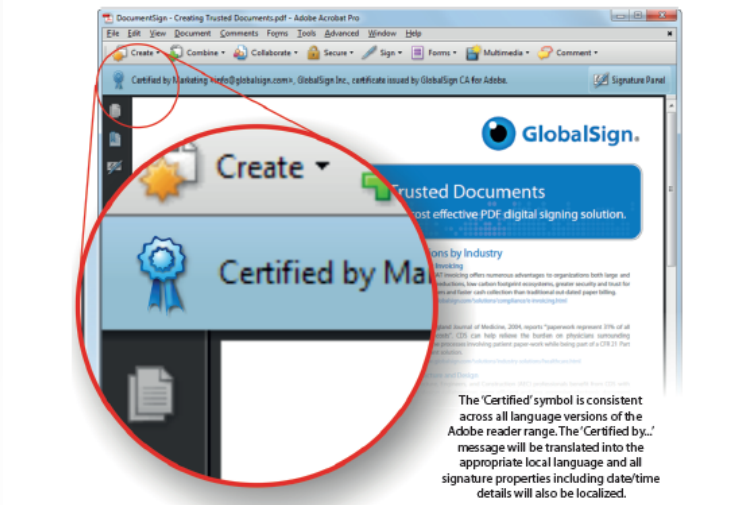
Subscription Fees of e-Cert (Organizational "Mutual Recognition" Status)

New/Renewal Subscription Fee	<u>Certificates with a 1-year validity period</u>	<u>Certificates with a 2-year validity period</u>	<u>Certificates with a 3-year validity period</u>
New application or renewal	HK\$150 per certificate	HK\$300 per certificate	HK\$450 per certificate
Administration fee (irrespective of the number of Authorised Users)	HK\$150 per application	HK\$300 per application	HK\$450 per application
	The Administration Fee is as the price of the longest validity e-Cert if the application form contains applications for variety validity certificates.		
e-Cert Token Fee	e-Cert (Organizational) with "Mutual Recognition" Status is mandatory to storage in separate e-Cert Token at a price of HK\$290 each.		

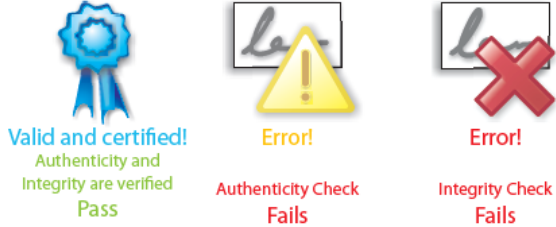
Example:

- 3 years token =
\$450 application + \$450 admin fee
+ 290 USB Token fee
- Total: \$1190 per user for 3 years
- Around \$396.7 per year per user

5. Validation of Document



Following a thorough verification of the 'Applicant' requesting a PDF Signing for Adobe CDS certificate, GlobalSign will issue a 'pickup' link which allows a certificate to be generated and securely stored on a SafeNet® hardware cryptographic device. Authors can digitally certify PDFs using certificates "chained" up to the trusted Adobe Root. Recipients simply need to open the document using the Adobe free reader to instantly verify the authenticity and integrity of the document. Adobe's simple to interpret "Blue Ribbon, Yellow Warning Triangle, and Red X" trust messaging allows even novice users an easy to understand method to determine if the document is legitimate.





Valid and certified!

Authenticity and Integrity are verified

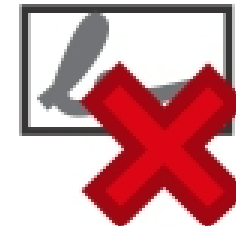
TRUST



Error!

The author cannot be verified

DO NOT TRUST



Error!

The document has been modified since it was signed

DO NOT TRUST

CHECK INTERNET CONNECTIVITY



Certified by [redacted] 有限公司, [redacted] 有限公司 (0002248920, 107478280011220100180054, [redacted] LIMITED, [redacted] LIMITED), certificate issued by Hongkong Post e-Cert CA 2 - 15.

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

Hongkong Post Root CA 2
Hongkong Post e-Cert CA 2 - 15

Summary Details Revocation Trust Policies Legal Notice



[redacted]

[redacted] 公司 [redacted] 公司

Issued by: Hongkong Post e-Cert CA 2 - 15
Hongkong Post

Valid from: 2021/01/22 16:15:08 +08'00'

Valid to: 2024/01/22 16:15:08 +08'00'

Intended usage: Digital Signature, Non-Repudiation, Client Authentication, Email Protection

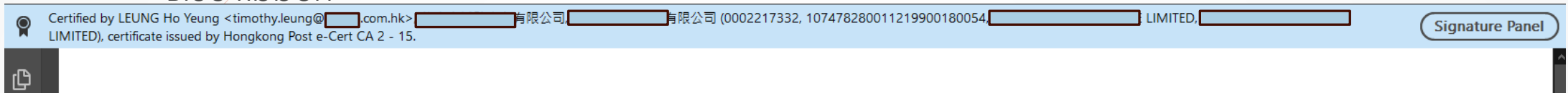
Export...

Demo Reports

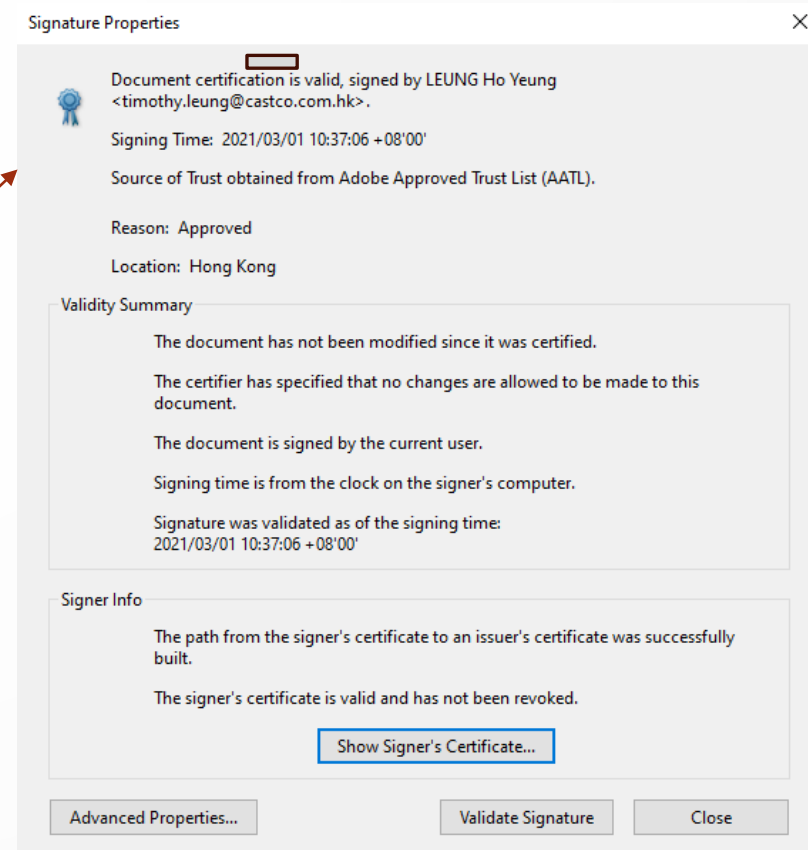
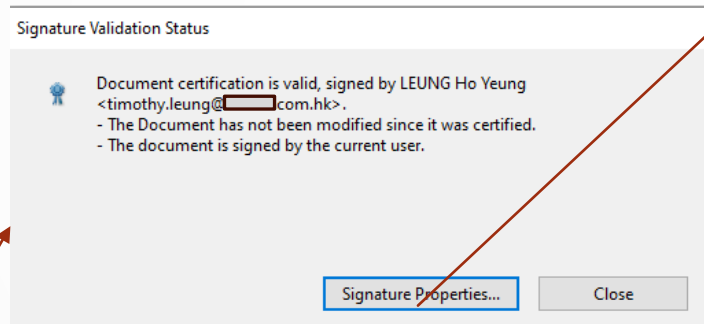
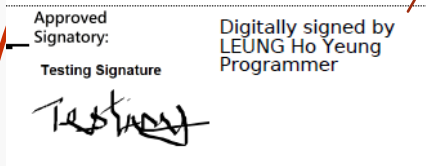


➤ Digital signature

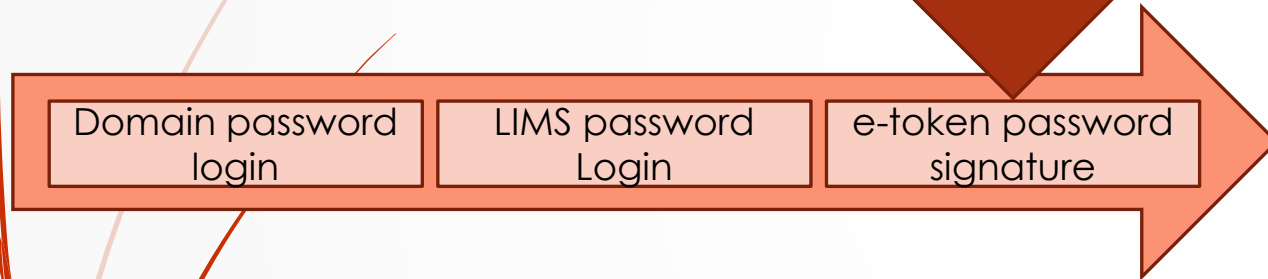
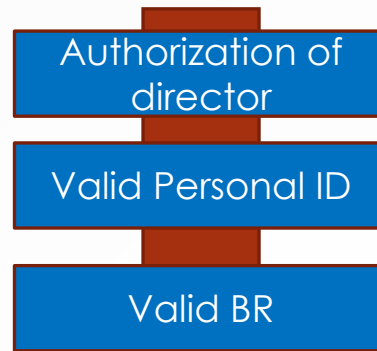
➤ Blue ribbon



➤ Signature info



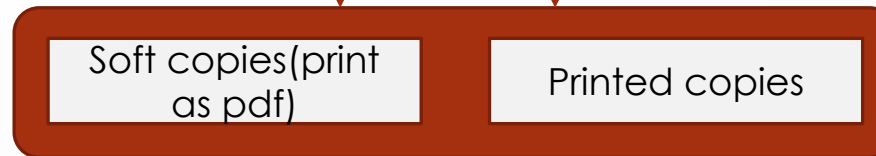
Layers of authentication



Original PDF (Kept in Company Database)

Soft copies (Valid Copies with digital signature)

Valid Copies !!



Invalid Copies



Digital signature

AC
ML

1. Document is **locked** and no further changes can be made
2. **Blue ribbon status** summary when opening with Adobe reader

Can and Cannot after Signing

- You can rename file
- You can copy and paste
- You can email
- You cannot Print to PDF
- You cannot combine or split the PDF

Test Report
on Compressive Strength of Concrete Cubes
 Test Method: CS1:2010 Section 12 + Amend. 1/2013

Internal No. Test Report No.
 Page 1 of 1 page(s)

Sample Details as Supplied by Customer:

Customer:
 Address:
 Project / Site:
 Location in Batch Sample:
 Supplier:
 Source of concrete:
 Cement brand:
 Concrete Mix:
 Concrete Grade:
 Cement Content:
 PFA/GGBS:
 Date of Sample:
 Time of Sample:
 Source of aggregate:
 Method of Casting:
 Site Curing:
 No. of cubes:

Supply Method:
 Source of admixture:
 Admixture Dosage:
 Design:
 W/C ratio:
 PFA/GGBS:
 Time of placement:
 Place of casting:
 Name of contractor:
 Max./Min. Nominal:

Certificate of Sampling, Slump Test, Cube Making and Curing:

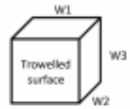
Certificate of sampling, slump test, cube make and curing

Laboratory Information and Test Results:

Date Received:
 Curing Method:
 Test Location:

RFID Tag No. / Security label No.	
Identification no. of cube	Cube mark
	Lab Ref. No.
Mould no.	
Condition on received*	
Edges/corners damaged**	
Dimensions	W1 - width 1 <input type="text"/> mm W2 - height <input type="text"/> W3 - width 2 <input type="text"/>
Mass	as received <input type="text"/> kg saturated in air <input type="text"/> in water <input type="text"/>
Density***	by calculation <input type="text"/> kg/m ³ by water-displacement <input type="text"/> kg/m ³
Load at Failure	<input type="text"/> kN
Compressive Strength****	<input type="text"/> MPa
Type of fracture*****	<input type="text"/>

Notes: * N - Normal, H - Honeycombing, P - Poor Compaction, I - Irregular Shape, O - Oversize
 U - Undersize, D - Surface Dry, W - Surface Wet, M - Immersed in Water
 Y - for cubes having broken edges/corners with a dimension of 20mm or more in any direction
 ** N - for cubes without broken edges/corners or having broken edges with a dimension less than 20mm in any direction
 *** Determination of density is in accordance with CS1:2010 Section 16.
 **** Compressive strength is based on measured loaded cross-sectional area (W1 x W2).
 ***** S - Satisfactory failure, U - Unsatisfactory failure (Please specify Pattern Number by referring Figure 13 in Section 12 of CS1:2010.
 If the failure pattern cannot be found in Figure 13, the laboratory is required to record the unusual fracture.)
 All test results relate only to the sample(s) tested.



Remark:

Checked By:

Approved Signature: Digitally signed by
 Manager
 Date of Issue:

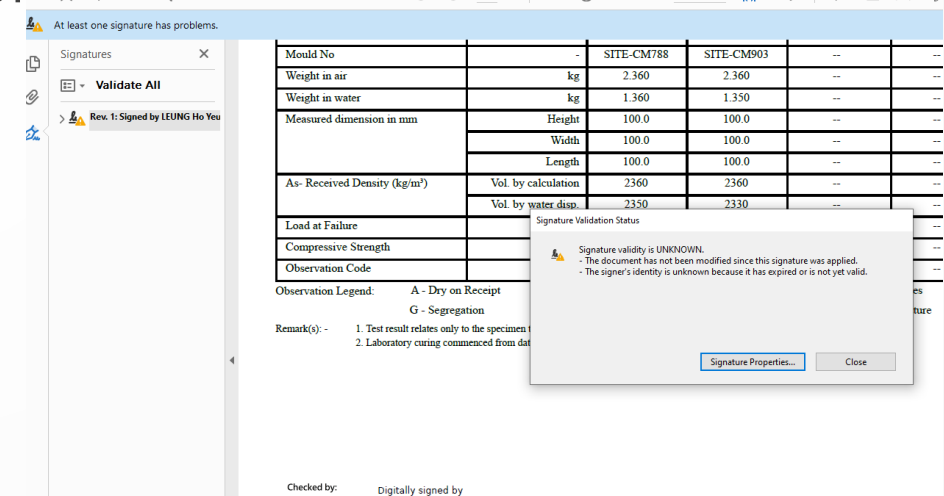


A decorative graphic is located on the left side of the slide. It features a vertical orange bar on the far left, a horizontal orange arrow pointing right, and several thin, curved lines in shades of orange and red that sweep across the page from the bottom left towards the top right.

6. Points to Note

Note:

- Q: Can you still digitally sign the report after the certificate expired
- A:
 1. Unfortunately, yes! You can still sign the report
 2. Adobe / other pdf reader will show warninas with expired cert alert

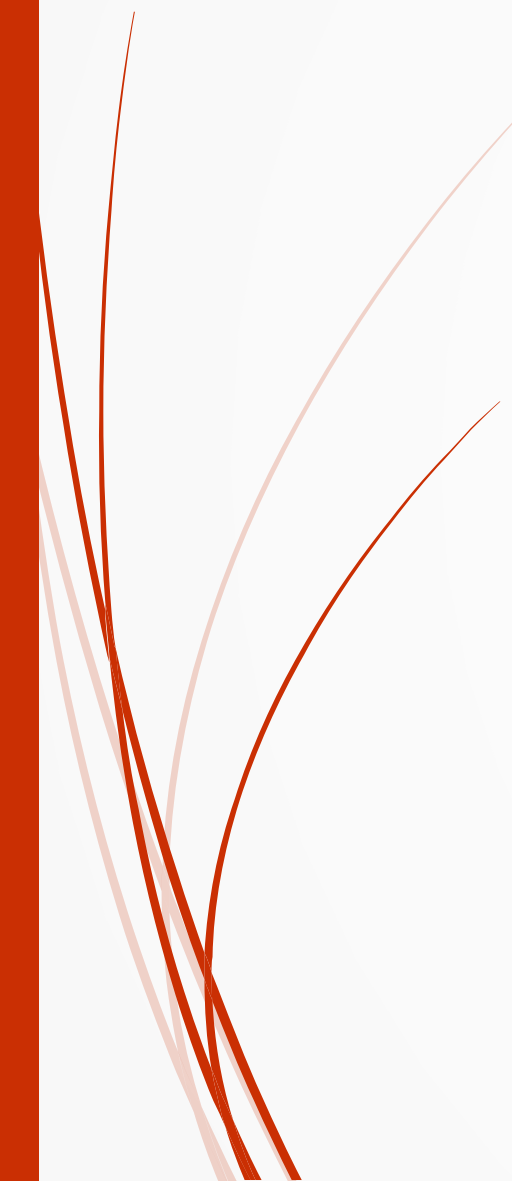


Note:

- Q: What do we do if the signer left the company or token is lost?
- A: Request Revocation from Hong Kong post



Note:

- Q: Why would a Digital Certificate expire?
 - New certificate can be issued with the latest security standards.
- 

Benefit

- Improve efficiency
- Save storage space
- Save paper and printing cost
- Save Environment



AC
ML

**Let's Save the World
and
Go Digital.
Thank you.**