OVERVIEW
OF DOCUMENT SECURITY

Thio Fu Wang
Director, eSecurity Centre of Excellence
Government confirms leaked document on PKFZ as official

By Shazwan Mustafa Kamal

KUALA LUMPUR, Dec 2 — The government lodged a police report recently about leaked Cabinet documents on the ongoing Port Klang Free Zone (PKFZ) scandal.

In a written reply to Klang MP Charles Santiago, the home affairs minister stated that the police report was made by the Finance Ministry on Sept. 16, 2009, and that the case was still being investigated by the police.

The case has been classified under section 8 of the Official Secrets Act (OSA) where a person can be charged with divulging official government secrets in a wrong manner.

"The government will not hesitate to take strict action against any party which leaks out official government secrets either through government agencies or other means, based on the legal provisions at hand."

A thorough criminal investigation is under way to determine the source of the leaked document, whether it was a technical glitch, carelessness or a "hidden culprit."

In lodging a police report, the government is conceding the fact frequently stated by Barisan Rakyat that the leaked documents are indeed official Cabinet papers on the PKFZ issue.

The government has also announced that it has appointed a special task force led by its Chief Secretary to look into the Auditor-General's report on the PKFZ.

The leaked Cabinet documents originally surfaced on the online web portal Malaysia Today some months back.

The contents are said to suggest that the Cabinet had been aware of the financial losses faced by PKFZ for some time, and no follow-up action had been taken to remedy the situation.
OVERVIEW OF DOCUMENT SECURITY

An organisation’s documents are critical to accomplishing its mission and achieving its goals.

Document Security provides protection from unauthorized access, leakage, modification, and replication.

Document Security covers the security of both Hardcopy and Softcopy documents.
CLASSIFICATION OF DOCUMENT SECURITY

- **Hardcopy Document Security**
  - Hardcopy Security Features
  - Document Lifecycle Management
  - Secure Printing
  - Document Leakage Protection
  - Document Integrity Assurance (e-Signature)

- **Softcopy Document Security**
DOCUMENT LEAKAGE SOURCES

Confidential Data

Leakage Channels
## Modes of Attack on Hardcopy

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeiting</td>
<td>Unauthorized reproduction of a document, typically using optical means such as photocopying.</td>
<td>Similar documents containing identical data, both appearing authentic.</td>
</tr>
<tr>
<td>Tampering</td>
<td>Unauthorized modification of a document, e.g. to change sensitive data.</td>
<td>An inauthentic document containing invalid data.</td>
</tr>
<tr>
<td>Imitation</td>
<td>Unauthorized creation of an authentic-looking document. Typically done via tools such as Photoshop.</td>
<td>An inauthentic document that may contain arbitrary or valid data.</td>
</tr>
<tr>
<td>Origination</td>
<td>Unauthorized printing of a document through the actual system, possibly by disgruntled staff.</td>
<td>Multiple copies of an authentically-printed document that cannot be distinguished from each other.</td>
</tr>
<tr>
<td>Leakage</td>
<td>Unauthorised disclosure of confidential document</td>
<td>Breach of confidentiality</td>
</tr>
</tbody>
</table>
THE NEED FOR HARDCOPY SECURITY

Despite technological advances, the printed page is still the predominant form of trusted communication.

Unfortunately, the printed document is inherently insecure: **firewalls** and **passwords** do not apply in the hardcopy space.

63% of businesses have experienced paper-related data breaches*

* Source: Quocirca Report, February 2013
Research carried out by Quocirca among 150 large enterprises in the UK, France, and Germany. Respondents were asked, “Has your business ever suffered a print-related data breach?”

From “Printing: A False Sense of Security?” published by Quocirca, Feb 2013
POTENTIAL SOLUTIONS FOR HARDCOPY SECURITY
Phidélity is a document security product that helps to protect the organisation from counterfeit, forgery and disclosure of hardcopy printouts.
Phidelity provides multi-layer complementary security features to protect the hardcopy document
# Inspection for Document Authenticity

<table>
<thead>
<tr>
<th>First Line Inspection</th>
<th>Human only verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Line Inspection</td>
<td>Human with tools</td>
</tr>
<tr>
<td>Third Line Inspection</td>
<td>Human with more sophisticated tools</td>
</tr>
</tbody>
</table>

**Source:** European Conference on Security and Detection, 28-30 April 1997
Conference Publication No. 437
# PHIDÉLITY FEATURES

## Optical Watermark

<table>
<thead>
<tr>
<th>9 Marks &amp; Numbers</th>
<th>10 No. &amp; Kind of Packages</th>
<th>11 Quantity &amp; Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1258/3658</td>
<td>MMM 97, CTNS 1345 PCS (115.5 NZ) 345.45 KG ladies 100% polyester jumper wearing apparel Purchase order item E34512 017-345 E34562 017-344 E34567 017-346</td>
<td>100 KGS</td>
</tr>
<tr>
<td>001/05343</td>
<td>97, CTNS 1235 PCS (115.5 NZ) 678.5 KG mens 100% cotton knit jacket (sleeve less) wearing apparel Purchase order item E34512 017-345 E34562 017-344 E34567 017-346</td>
<td>100 KGS</td>
</tr>
</tbody>
</table>

Sample Certificate
### PHIDÉLITY FEATURES

**Transactional Micro-print**
- 2nd line inspection
- Very fine print
- Dynamic Information
- Provides Accountability

<table>
<thead>
<tr>
<th>Inspection Level</th>
<th>Type of Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Line Inspection</td>
<td>Human only</td>
</tr>
<tr>
<td>Second Line Inspection</td>
<td>Human with tools</td>
</tr>
<tr>
<td>Third Line Inspection</td>
<td>Human with more sophisticated tools</td>
</tr>
</tbody>
</table>
PHIDÉLITY FEATURES

• CryptoMark
  – 2\textsuperscript{nd} line inspection
  – Visually Encrypted
  – Provide Document Authenticity
PHIDÉLITY FEATURES – CRYPTOMARK

• Benefits
  – Relatively low-cost, without any additional complex equipment to verify the document authenticity.
  – Verification Lens can be specific to an organization or at department level.
  – Similar to other Phidélity features, it works by using Normal Paper, Ink and Printer.

• Applicability
  – Ideal for offline verification of document authenticity.
  – Suitable for IT-unfriendly environment, such as warehouse environment and remote rural areas where it is inherently difficult to have both Internet and PC setup readily available
PHIDÉLITY FEATURES

SecureCODE

- 3rd line inspection
- Detects document forgery

Exporters (Name & Address):
CrimsonLogic Pte Ltd
31 Science Park Road, The Crimson
Singapore 117611

Name: Fast Exporter Clerk
No: SCC-02-000001
Items: Ladies 100% polyester apparel 100Kgs

First Line Inspection
Human only verification

Second Line Inspection
Human with tools

Third Line Inspection
Human with more sophisticated tools

LSW9KAFD934K11MVALSDOR9
4JKFASKMSAS94QK409ERT340Y
3L5OPE408QFOLOFOLEDFPSF95
ZKV044KPE4RMFJRN345MV0B
MPO99F81KPT8Q3OF894V9141
NG45MBQ379D09T04Z8TMD0
ALSDUHAL5I98ASDFHA031BOI
Items: Ladies 100% polyester apparel 100Kgs
PHIDÉLITY FEATURES

• Verification Channels
  – 2D Barcode Gunner/Reader

<table>
<thead>
<tr>
<th>First Line Inspection</th>
<th>Human only verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Line Inspection</td>
<td>Human with tools</td>
</tr>
<tr>
<td>Third Line Inspection</td>
<td>Human with more sophisticated tools</td>
</tr>
</tbody>
</table>

Exporter (Name & Address):
CrimsonLogic Pte Ltd
31 Science Park Road
The Crimson
Singapore 117611

Name: Fast Exporter Clerk
No: SCC-02-000001

Items: ladies 100% polyester apparel 100Kgs
PHIDÉLITY FEATURES

• Verification Channels
  – 2D Barcode Gunner
  – Email
  – Web page
  – Pocket PC
  – Software client
PHIDÉLITY FEATURES

ID-Trace
- 3rd line inspection
- Embed user information into document
- Steganography
- Accountability

<table>
<thead>
<tr>
<th>First Line Inspection</th>
<th>Human only verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Line Inspection</td>
<td>Human with tools</td>
</tr>
<tr>
<td>Third Line Inspection</td>
<td>Human with more sophisticated tools</td>
</tr>
</tbody>
</table>
PHIDÉLITY FEATURES

Objectives

- Works by using Normal Paper, Ink and Printer.
- Embeds fingerprint of user for Accountability and Traceability.
- Minimal overhead to the existing printing process
- Resilience to the daily document handling process (Faxed, copied, folded etc)
- Fingerprint is covert and not easily removed from paper or tampered.
PHIDÉLITY FEATURES

• Print Control
  – Centralized Control
  – Dynamically optimizes printer settings
  – Limits number of copies
  – Restricts Virtual Printer Driver
  – Minimal client footprint installations
PHIDÉLITY FEATURES

**ID-Trace**
Anti-disclosure feature: embeds user fingerprint on the page for accountability.

**SecureCode**
Anti-forgery feature: Secures a barcode holding digitally signed sensitive information.

**Optical Watermark**
Anti-copy feature: first-line visual inspection.

**CryptoMark**
Anti-forgery feature: holding visually encrypted information.

**CrimsonLogic**
Anti-disclosure feature: holds visually encrypted information.

**Transactional microprint**
Anti-copy feature: fine dynamically-generated text.

---

**INVENTION DISCLOSURE – (DOC)**

In terms of the Intellectual Property Policy, members of the MRC are obliged to disclose any newly created or discovered IP to the MRC IC, and to cooperate with the IC in all matters, including technical, marketing, patenting and licensing. The form for reporting IP is entitled MRC IC Invention Disclosure Form and may be downloaded here. The form provides the information needed to start assessing the patentability and commercial opportunity for the invention. IP Creators must inform their project supervisor, department head or unit director, and the technology transfer office associated with or designated authority at the University, for external MRC Research Units only, of any invention disclosures and other documents.

1. **Terms and conditions**
   The general procedure for disclosure and commercialization of IP is shown in the figure and discussed in more detail below. It is important to note that the MRC recognizes the right of IP Creators to participate in decisions regarding the commercialization and use of IP generated by them. IP Creators are therefore entitled to full disclosure of the status of the IP and will be advised before the MRC enters into any contracts for the commercial and any other related work.

2. **Submission**
   Submission of an MRC IC Invention Disclosure Form by MRC members. MRC IC Invention Disclosure Forms must be submitted by email or post, hardcopy and a disc, to the MRC IC and, in the case of external MRC units, groups and centers, to the technology transfer office associated with or designated authority at the relevant university. If emailing the form to us, please ensure that the Invention Disclosure document is password-protected, since email is generally not secure and sending unprotected documents via this route may amount to a public disclosure, which will render the invention as described as unpatentable.

3. **Documents**
   MS Word documents can be password-protected by opening the document and clicking on Tools and Options. In the Options window click on the Save tab near the bottom of this window there is an option to insert a Password to open. Type in a password of your choice in the space provided. You will be prompted to retype the password, then click OK. Once you close the document, you will not be able to reopen it without the password.
Phalanx is an end-to-end Print Lifecycle Management System that provides:

- Print Job Logging and Snapshots
- Dashboard & Reports
- Batch Verification
- Auditing
- Document Lifecycle Tracking
- Notification
- Authenticated Pull Printing
AUTHENTICATED PULL PRINTING

The ability to ask someone to validate their identity before allowing the use of specific device functions

- Card-based
  - Proximity badge authentication
  - Smart card authentication

- LDAP authentication

- Dual authentication with proximity card and smartcard
# Modes of Attack on Softcopy

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering</td>
<td>Unauthorized modification of a document, e.g. to change sensitive data.</td>
<td>An inauthentic document containing invalid data.</td>
</tr>
<tr>
<td>Imitation</td>
<td>Unauthorized creation of an authentic-looking document. Typically done via tools such as Photoshop.</td>
<td>An inauthentic document that may contain arbitrary or valid data.</td>
</tr>
<tr>
<td>Leakage</td>
<td>Unauthorised disclosure of documents which are classified as confidential or above.</td>
<td>Loss of sensitive information can be very costly in terms of tarnished brand image, reputation, weakening of competitive edge, regulatory fines, lawsuits or lost of opportunities.</td>
</tr>
</tbody>
</table>
SOFTCOPY LEAKAGE SOURCES

- Internet/Web
- Portable Recordable Media
- Email
- Personal Computer
POTENTIAL SOLUTIONS FOR SOFTCOPY SECURITY
BASIC OF SOFTCOPY DOCUMENT SECURITY

Authentication
- 1-Factor / 2-Factor Authentication

Authorisation
- Access Based on Need-to-Know Basis

Audit Trail
- Record the Activities Log for Subsequent Verification

Confidentiality Protection
- Password-protection / Encryption
ELECTRONIC SIGNATURES

Signing a softcopy document typically involves printing the document, penning a signature, scanning the document, and emailing it back to the concerned party.

Electronic signatures prove the origin of a softcopy document without the need for a handwritten signature.

Depending on the implementation, they can also ensure the integrity of the document, i.e. prove that the document has not been altered.
## TYPES OF ELECTRONIC SIGNATURES

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digitized signatures</strong></td>
<td>• Image-based versions of normal handwritten signatures, captured using optical means or via a hardware capturing device and embedded in the document.</td>
</tr>
<tr>
<td><strong>Biometric signatures</strong></td>
<td>• Hash value representations of biometric measurements such as fingerprints, hand geometry (finger lengths and palm size), iris patterns, or retinal patterns, collected using electronic sensors and attached to the document file.</td>
</tr>
<tr>
<td><strong>Digital (cryptographic) signatures</strong></td>
<td>• Mathematical signatures based on asymmetric cryptography. The issuer’s private key is used to sign a document and the issuer’s public key is used for verification. Provides authentication as well as integrity verification.</td>
</tr>
</tbody>
</table>
INDUSTRY PLAYERS

DocuSign - Google-backed signature service

Sertifi - Accepts up to 300 different file types including Word, Excel and PDF.

Adobe EchoSign - Acquired by Adobe in 2011. Well integrated with Adobe products

RightSignature - Recently acquired by Citrix Systems
DATA LOSS PREVENTION

Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis

The key defining characteristics are:

- Deep content analysis
- Central policy management
- Broad content coverage across multiple platforms and locations

Reference: www.securosis.com
INDUSTRY PLAYERS

- Symantec
- McAfee
- WebSense
- TrustWave
- Trendmicro
- Fidelis Security Systems,
- GTB Technologies
- Code Green Networks
- RSA
DOCUMENT SECURITY
SPECTRUM
DOCUMENT SECURITY SPECTRUM

**DOCUMENT CREATION**

- Desktop Applications
  - Various Desktop Applications
  - Multiple Input Sources
  - Multiple Document Formats
  - Textual Information
  - No change to document creation process

- Data Leak / Loss Protection (DLP) System
  - Document in digital format
  - Document Access on a Need-to-Have basis
  - Data loss / leak via softcopy is controlled

**SOFTCOPY CONTROL**

- Document Management System (DMS)
  - Phidélity & Phalanx

**HARDCOPY CONTROL**

- Print Access Restriction
  - Restrict printing on a Need-to-Have basis
  - Metering and Charge-back
  - Embeds security features onto printouts
  - Normal printer, paper & ink
  - Transparent and minimal print overhead
  - Authenticated pull-printing

- Distribution Control
  - Closed environment
  - Restrict duplication and distribution
  - Anti-counterfeiting and anti-forgery security

- Traceability
  - “Fingerprint” on document is recovered
  - Traceability persists over time
  - Resilience to daily document handling
  - Culture of responsible and accountable printing

**Print Access Restriction**

- **Fax**
  - ID-Trace Phalanx

- **Scanner**

- **Copier**

**Distribution Control**

- **Fax**

- **Scanner**

- **Copier**

**Traceability**

- **ID-Trace Phalanx**
What Document Security Threats Does Your Organization Face?
Thank You

Fu Wang, Thio
fuwang@crimsonlogic.com