

香港民意研究所（研究所，PORI）有關 普及投票系統資訊安全之聲明

2020 年 7 月 17 日

香港民意研究所謹代表普及投票系統的資訊科技顧問小組，向公眾闡述有關系統的資訊安全，以及說明過去幾天與系統保安相關的事故。

普及投票系統設計以安全及保密作首要考慮，只收集最低限度的個人資料，包括香港身分證的最後四碼、發出日期及出生日期，以作核實身份、防止重覆投票之用。為防止洩露個人資料，系統不會以明文傳送任何資料。所有個人資料均先以單向密碼雜湊處理，再進行端對端加密，然後以 QR Code 形式傳送至票站設備。票站設備鑰匙只能解密指定資料作核實身份之用，核實身份後再傳送已加密的選票資料至伺服器。進行點票時，伺服器的資料會經加密網絡下載，以 USB 隨身碟轉移至離線電腦上進行解密及點票。為避免遭黑客經互聯網入侵，電子點票系統與互聯網完全隔絕，並且移除或停用了不必要的硬件。點票所使用的解密鑰匙經由多名人員妥善保存於不同地點，整個點票系統包括離線電腦，均獨立於研究所辦公室的電腦系統。

有關初選系統的技術規格可參考研究所早前公佈之 [GitHub](#) 連結，稍後技術團隊亦將開放源碼，希望可以為各公民團隊所用，並協助繼續發展系統。開放源碼亦可以讓任何人士均可審視程式碼，將來再使用系統時，協助儘早指出並堵塞任何可能存在的保安漏洞。

我們當初已經假設可能會有其他組織（包括政府）監控通訊網絡或入侵電腦。不過作為一個民間組織，在有限的資源下要作出防禦的難度甚高；所以我們從投票系統設計中已設置多重保安，保證系統洩漏個人資料的可能性極低。簡而言之，電子投票系統有三個重要部分需要重點保護：

- 離線處理的電腦和物理環境要保證安全
- 解密鑰匙需要妥善的離線保護
- 每個票站均需設有一組獨立的加密鑰匙和密碼，以防止大規模資料洩露

就我們所知，在整個初選的運作當中，電子投票系統之各個部份均正常運行，點票過程亦在研究所以及資訊科技顧問小組的監察下進行。另外紙張點票的流程與環境也是重要一環，不過相對獨立於電子投票，我們不在此詳述。

所有原始資料，包括個人資料及解密鑰匙均已在點票完成後銷毀；包括：

- 刪除伺服器上的投票檔案資料庫及其所有備份
- 所有曾經儲存解密鑰匙及投票檔案的 USB 以重覆寫入方式刪除
- 兩部曾經儲存少量紙張點票資料的手提電腦硬碟以重覆寫入方式刪除

研究所僅保存不含個人資料之統計數據作日後各方研究之用，統計數據已被加密及封存，待九月立法會選舉後公開。

最後，我們也希望藉此向公眾解釋及交代較早前發生兩件與資訊保安相關的事故：

一、電子點票結果提前被傳媒披露

研究所仍在調查事件，顧問小組暫不認為與投票系統有關。據我們了解，當晚系統點票完畢，點票結果經視像會議讀出，並由研究所職員紀錄於 Google Spreadsheet 及文件中以供內部使用。文件只紀錄有關點票結果，並不存在任何選民的個人資料。至於是次處理文件的方式是否存在瑕疵，令黑客有機可乘或資料被流出，則有待進一步跟進調查。

我們再一次強調，投票資料及解密鑰匙均為離線處理，據我們所悉並無外洩。

二、上週五晚間研究所曾被警方搜查，系統需重設加密鑰匙

當晚顧問小組得悉，其中一部被警方搜查的電腦儲存了所有票站加密鑰匙及密碼。雖然警方保證資料並不會用於調查以外之用途，但鑑於我們無法保證所有票站的加密鑰匙及密碼均能妥善保密，謹慎起見，星期五當晚即決定使用新的離線電腦重設所有加密鑰匙，並安排將離線電腦及解密鑰匙，交由保密人員於安全地點保管。此措施導致：

- 週六的票站需要延遲開始
- Android 投票 App 無法使用，用戶只可透過網頁版投票 (iPhone 投票 App 因未通過 Apple 的審查，仍維持網頁版投票)

帶來不便，還望體諒。

我們會繼續秉持對資訊保安的最高要求，保障個人資料安全，希望繼續協助香港人在安全的環境下表達意見。