

# 可驗證憑證(Verifiable Credentials) 2.0 於2025年5月15日發佈

## 使數位憑證的表示、交換和驗證變得更容易、更安全

提供以加密安全、尊重隱私和機器可驗證的方式來表示數位憑證的機制，以及允許特定應用（如身份憑證、大學憑證）使用其各自專業用語的擴展機制。

憑證持有者可將憑證出示給驗證者，驗證者可驗證該聲明是否確實來自發行者，且未被篡改。可驗證憑證的真實性和完整性是透過使用密碼技術，特別是使用數位簽章和相關數學證明，來檢查其內容的結構有效性。這樣的機制可確保發行者、持有者和驗證者三方，能對所提供或接收的資料有一致的信任機制。



可驗證憑證的持有者也可以提供憑證中的部分資訊給驗證者（即選擇性揭露私人資料），或是將多個憑證合而為一。這些所謂的「可驗證出示」通常是短期的，並不打算長期儲存。不過，系統中也內建了讓過期憑證可以更新的機制。簽章和加密所使用的標準，是基於生態系統中廣泛採用的加密方法之上。

這是一種可讓第三者驗證和確認您的個人憑證（不只是人）是否正確的機制。

在日本的COVID-19 疫情期間，就曾推出可透過智慧型手機簽發疫苗接種證明。

此外，VC技術也被考慮應用在供應鏈中，例如貿易，在這種供應鏈中，需要在許多利益相關者之間安全地交換準確的資訊。

此外，在貿易

等的供應鏈管理等領域，因為涉及多方利害關係人之間安全地進行準確的資訊交換，因此目前也在評估導入VC技術的可能性。

另一方面，同樣應用於VC的DID也稱為分散式ID，它是取代傳統由企業集中管理帳號／密碼的方式，讓個人自行管理自己的ID，並只與需要者分享必要資訊的架構。

例如，加州的DMV（駕駛執照系統）利用DID驗證證書，用於識別發行人和持有者的裝置；截至2024年9月，已新增600,000個，即每天1,200個。



Verifiable Credentials Working Group: <https://www.w3.org/groups/wg/vc/>

Verifiable Credentials Data Model v2.0 規格: <https://www.w3.org/TR/vc-data-model-2.0/>

