GTIDEM JS Library

Contents

Revision History

A revision occurs with each release of the product, or as needed. A revised version can contain minor or major changes. Table 1 lists the versions of this manual.

Table 1. Revision History

Revision	Description	Date
1.0	First release。Define functions and status code.	**08/20/2021**

1. 概述

描述 GTIDEM JS 的行為，定義名詞和解釋狀態碼的意義

2.名詞解釋

GTIDEM JS	Javascript library, 在瀏覽器上使用 webauthn API 與載具溝通。
Label	儲存在載具中，可作為搜尋特定憑證或是金鑰的條件。
Key ID	由使用者指定，在建立金鑰對或匯入憑證使用。之後當作Label 使用。
Key Handle	使用者未指定 Key ID 時，由載具產生此值。之後可當作Label 使用。
CSR	Certificate Signing Request

2. 函式

2.1函式概述

名稱	描述
GTIDEM_SignDataByIndex	使用特定位址金鑰對資料簽名
GTIDEM_SignDataByLabel	使用特定標籤金鑰對資料簽名
GTIDEM_ReadCertByIndexWithoutPIN	不需要驗證使用者密碼就可讀取特定位址憑證。
GTIDEM_ReadCertByLabelWithoutPIN	不需要驗證使用者密碼就可讀取特定標籤憑證。
GTIDEM_GenRSA2048	產生RSA 2048 金鑰對並返回公鑰
GTIDEM_GenRSA2048CSR	產生RSA 2048 金鑰對並返回CSR 格式
GTIDEM_ImportCertificate	匯入憑證
GTIDEM_DeleteCertByLabel	刪除指定標籤的憑證和金鑰對
GTIDEM_ClearToken	清除卡片中的所有憑證和金鑰對
GTIDEM_ChangeUserPIN	修改使用者密碼
GTIDEM_GetTokenInfo	返回載具資訊

2.1. 函式說明

2.1.1. GTIDEM_SignDataByIndex

GTIDEM_SignDataByIndex(index, bSerialNumber ,alg_number, bPlain)

使用特定位置的金鑰對傳入的資料做簽名。

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.signature	簽名

2.1.2. GTIDEM_SignDataByLabel

GTIDEM_SignDataByLabel(bLabel, bSerialNumber ,alg_number, bPlain)

使用指定標籤的金鑰對傳入的資料做簽名。

參數		
Uin8Array	bLabel	指定標籤的金鑰對
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列
Number	alg_number	簽名演算法, ALG_RSA2048SHA256 或者 ALG_RSA2048SHA256_PreHash
Uin8Array	bPlain	被簽名的資料

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.signature	簽名

2.1.3. GTIDEM_ReadCertByIndexWithoutPIN

GTIDEM_ReadCertByIndexWithoutPIN(index, bSerialNumber)

不需要使用者密碼，就讀取特定位址的憑證。

參數		
Number	index	指定位址的金鑰對
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列
Number	alg_number	簽名演算法, ALG_RSA2048SHA256 或者 ALG_RSA2048SHA256_PreHash
Uin8Array	bPlain	被簽名的資料

參數		
Number	index	指定位址的憑證
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.certificate	憑證內容

2.1.4. GTIDEM_ReadCertByLabelWithoutPIN

GTIDEM_ReadCertByLabelWithoutPIN(bLabel, bSerialNumber)

不需要使用者密碼，就讀取特定標籤的憑證。

參數		
Uin8Array	bLabel	指定標籤的憑證
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.certificate	憑證內容

2.1.5. GTIDEM_GenRSA2048

```
GTIDEM_GenRSA2048(bSerialNumber, bKeyID)
```

產生 RSA 2048 金鑰對，並回傳公鑰的 RAW

參數		
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列
Uin8Array	bKeyID	用來綁定金鑰對，可填入 undefined 或是空陣列則載具會產生預設的 KeyHandle回傳。

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.keyhandle	若 bKeyID 有效，則此欄位為 undefined
ArrayBuffer	GTIdemJs.rsakeypair	公鑰的 RAW

2.1.6. GTIDEM_GenRSA2048CSR

GTIDEM_GenRSA2048CSR(bSerialNumber, bKeyID)

產生 RSA 2048 金鑰對並回傳 CSR 資料

參數		
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列
Uin8Array	bKeyID	用來綁定金鑰對，可填入 undefined 或是空陣列則載具會產生預設的 KeyHandle回傳。

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.keyhandle	若 bKeyID 有效，則此欄位為 undefined
ArrayBuffer	GTIdemJs.csr	CSR

2.1.7. GTIDEM_ImportCertificate

GTIDEM_ImportCertificate(bSerialNumber, bKeyHandle, bKeyID, HexCert, bPlain)

指定 KeyHandle 匯入憑證。若在 GTIDEM_GenRSA2048 或是 GTIDEM_GenRSA2048CSR 使用 KeyID綁定金鑰，則此處的 KeyHandle 要使用已指定的 KeyID。

參數		
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列
Uin8Array	bKeyHandle	指定欄位
Uin8Array	bKeyID	用來綁定金鑰對，可填入 undefined 或是空陣列則載具會產生預設的 KeyHandle回傳。
Uin8Array	HexCert	欲匯入的憑證內容

參數		
Uin8Array	bPlain	使用指定的金鑰簽名並用 ALG_RSA2048SHA256_PreHash 演算法對填入的資料簽名，所以資料長度必須為32 bytes，可做為確認憑證和金鑰對的匹配。若不需此功能，則可填入 undefined 或是空陣列。

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.signature	簽名

2.1.8. GTIDEM_DeleteCertByLabel

```
GTIDEM_DeleteCertByLabel(bLabel, bSerialNumber)
```

刪除特定標籤的金鑰和憑證。

參數		
Uin8Array	bLabel	指定標籤
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼

2.1.9. GTIDEM_ClearToken

```
GTIDEM_ClearToken( bSerialNumber)
```

清除載具中的所有憑證和金鑰。

參數		
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼

2.1.10. GTIDEM_ChangeUserPIN

```
GTIDEM_ChangeUserPIN(bOldPIN, bNewPIN, bSerialNumber)
```

修改使用者密碼。

參數		
Uin8Array	bOldPIN	舊密碼
Uin8Array	bNewPIN	新密碼
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼

2.1.11. GTIDEM_GetTokenInfo

```
GTIDEM_GetTokenInfo(bSerialNumber)
```

回傳載具資訊。

參數		
Uin8Array	bSerialNumber	指定序號序號。若不指定載具序號，則可填入 undefined 或是空陣列

回傳		
Number	GTIdemJs.statusCode	狀態碼
ArrayBuffer	GTIdemJs.fw	韌體版本
ArrayBuffer	GTIdemJs.sw	軟體版本
ArrayBuffer	GTIdemJs.pinRetry	剩餘密碼次數
ArrayBuffer	GTIdemJs.sn	載具序號
ArrayBuffer	GTIdemJs.rn	隨機亂數
ArrayBuffer	GTIdemJs.ecpoint	橢圓曲線公鑰

3. 狀態碼

狀態碼	名稱	描述
0x00	CTAP1_ERR_SUCCESS	成功
0x14	CTAP2_ERR_MISSING_PARAMETER	缺少必要參數
0x19	CTAP2_ERR_CREDENTIAL_EXCLUDED	憑證或是金鑰已經存在
0x20	CTAP2_ERR_CERTIFICATE_NOT_VALID	憑證或是金鑰不能使用
0x26	CTAP2_ERR_UNSUPPORTED_ALGORITM	不支援的演算法
0x28	CTAP2_ERR_KEY_STORE_FULL	內容已滿
0x2E	CTAP2_ERR_NO_CERTIFICATE	要求的憑證或是金鑰不存在
0x30	CTAP2_ERR_NOT_ALLOWED	不允許此操作
0x31	CTAP2_ERR_PIN_INVALID	驗證使用者密碼錯誤
0x35	CTAP2_ERR_PIN_NOT_SET	使用者密碼未設定或是需要修改使用者密碼
0x36	CTAP2_ERR_PIN_REQUIRED	需要驗證使用者密碼
0x38	ERR_TOKEN_EXPIRED	載具到期
0xF2	CTAP2_VENDOR_ERROR_TOKEN	載具序號錯誤
0xF2	CTAP2_VENDOR_ERROR_LENGTH	載具序號長度錯誤

4. 其他項目

4.1. Key Handle 的產生

當呼叫 GTIDEM_GenRSA2048 或是 GTIDEM_GenRSA2048CSR 而沒有指定 Key ID時，

載具會使用金鑰的 modulus 進行 SHA1 運算，取得其雜湊值當作 Key Handle 並回傳。