



JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

HPシンククライアント（Windows Embedded Standard 7 : WES7）でのXenDesktopスマートカードログオン

Ver.1.0

2013年1月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

目次

1. はじめに	4
1.1. 本書について	4
1.2. 本書における環境	4
1.3. 本書における構成	5
2. シンククライアント側の初期設定	6
2.1. Administrator での設定	6
3. Gléas での認証デバイスの準備	9
4. シンククライアントからのスマートカードログオン	10
5. 問い合わせ	12

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行した電子証明書と Gemalto .NET（ドットネット）製品を利用して、Windows Embedded Standard 7（WES7）を搭載したシンククライアント端末にてシトリックス・システムズ・ジャパン株式会社のXenDesktopで構築した仮想デスクトップへのスマートカードログオン環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- 【シンククライアント】日本HP 6360t Mobile Thin Client
Windows Embedded Standard 7 SP1 / Citrix Online Plug-in12.1.0.30
※以後、「シンククライアント」と記載します
- 【認証局】JS3 プライベートCA Gléas（バージョン1.10）
※以後、「Gléas」と記載します
- 【仮想デスクトップ基盤】Citrix XenDesktop 5 SP1 Express Edition / Microsoft Windows Server 2008 Standard SP2（64bit）
※以後、「XenDesktop」或いは「DDC」と記載します
- 【仮想デスクトップ】Microsoft Windows 7 Professional SP1
※以後、「仮想デスクトップ」と記載します
- 【認証デバイス】Gemalto .NETカード / PC USB-TR リーダ・ライター
※以後、「認証デバイス」と記載します

以下については、本書では説明を割愛します。

- Windowsスマートカードログオン環境のセットアップ
※弊社のWEBサイトでは、Windowsスマートカードログオン環境を構築するためのホワイトペーパーを公開しておりますので、構築時の参考にしてください

プライベート CA Gléas ホワイトペーパー
WES7 シンクライアントでの XenDesktop スマートカードログオン

参考URL : http://www.jcch-sss.com/images/Windows_Smartcard_Logon_Gleas_Configuration.pdf

- XenDesktop環境のセットアップ

※弊社のWEBサイトでは、XenDesktopでのスマートカードログオン環境を構築するためのホワイトペーパーを公開しておりますので、構築時の参考にしてください

参考URL : <http://www.jcch-sss.com/service/support/2011/12/citrix-xendesktop-smartcard-logon>

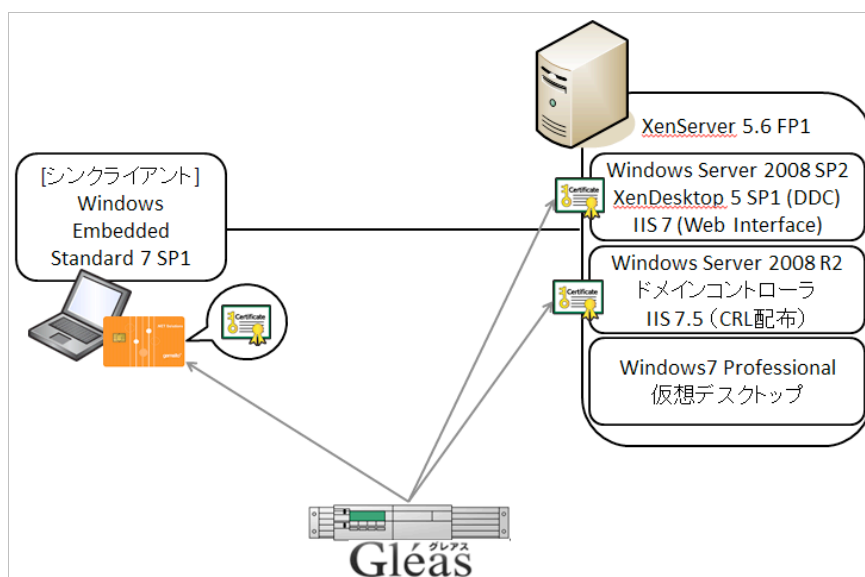
本環境では、上記ホワイトペーパーでのServiceサイトを利用しています

- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- シンクライアントやWindowsでのネットワーク設定等の基本設定
- 認証デバイスのパーソナライズ等の基本操作

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



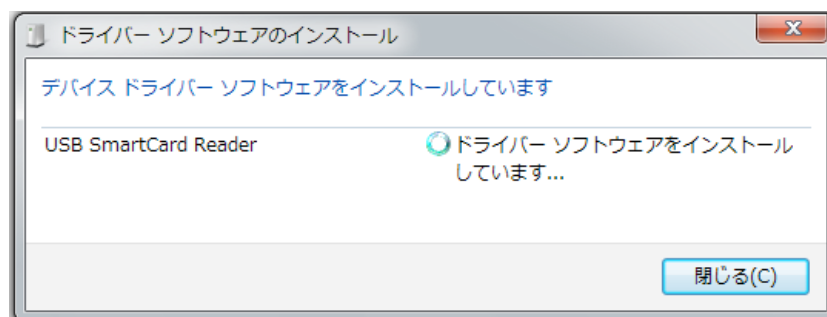
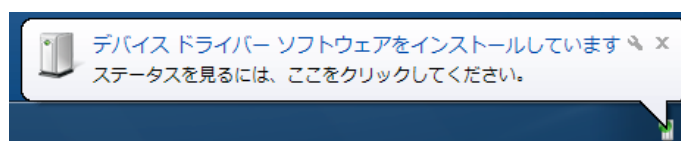
1. クライアント証明書は、Gléasより発行して認証デバイスに格納する
2. シンクライアントは、XenDesktopにスマートカードを用いてログインする
3. 事前設定された仮想デスクトップに転送され、その仮想デスクトップへのログオンにも認証デバイスを使用する（スマートカードログオン）

2. シンククライアント側の初期設定

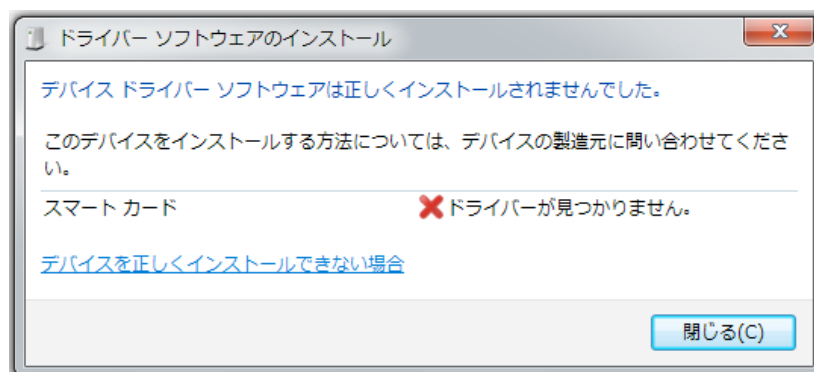
2.1. Administrator での設定

AdministratorでログインしEWF（Enhanced Write Filter）をオフにしてから以下の設定をおこないます。

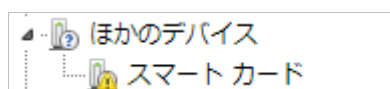
USB-TR リーダ・ライタをシンククライアントの USB ポートに挿入します。
シンククライアントは自動的にドライバをインストールします。



インストール完了後にカードを差し込むと、ドライバのインストールに失敗します。



デバイスマネージャーで見ると、スマートカードが認識されていないことが分かります。



プライベート CA Gléas ホワイトペーパー
WES7 シンクライアントでの XenDesktop スマートカードログオン

手動でドライバをインストールします。

ドライバファイルが必要になるので、マイクロソフト社の提供する「Windows Update カタログ」に Internet Explorer でアクセスします。

本ホワイトペーパー記載時での URL は以下の通りです。

<http://catalog.update.microsoft.com/v7/site/home.aspx>

検索ボックスに“Gemalto - Input - Gemalto Minidriver for .NET Smart Card” と入れて検索を行います。



検索結果が表示されます。

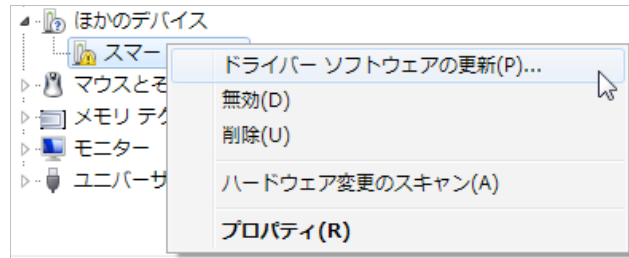
Minidriver と記載されているものがドライバになるので、[追加]をクリックしダウンロード用のバスケットに追加します。次に、「バスケットの表示」をクリックします。



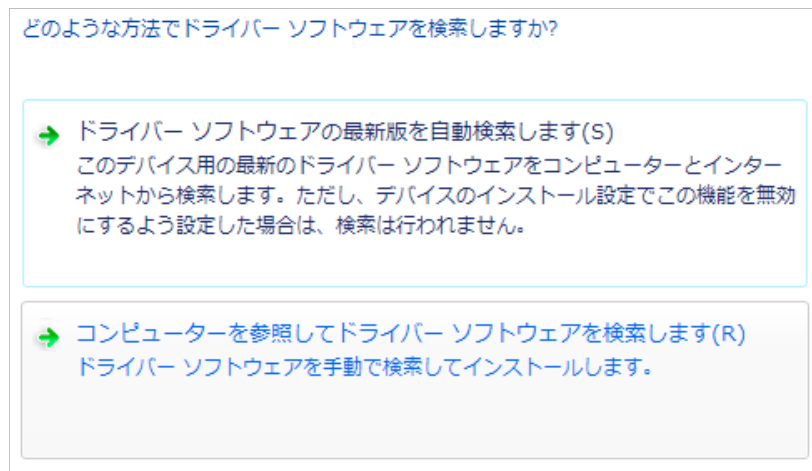
バスケットの中身が表示されるので、[ダウンロード]をクリックし CAB ファイル (.cab) をダウンロードします。終了後、CAB ファイルを展開します。

デバイスマネージャに戻り、[スマートカード]を右クリックし[ドライバーソフトウェアの更新(P)...]を選択します。

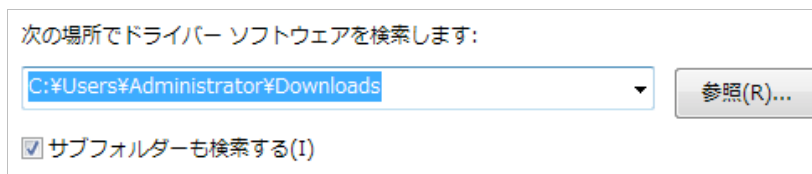
プライベート CA Gléas ホワイトペーパー
WES7 シンクライアントでの XenDesktop スマートカードログオン



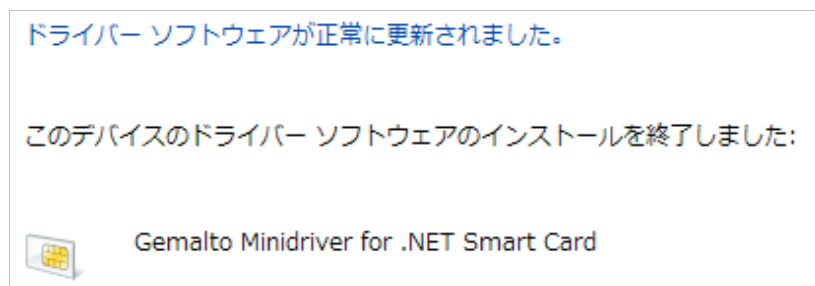
その後、ウィザードが起動するので[コンピューターを参照してドライバー ソフトウェアを検索します(R)]を選択します。



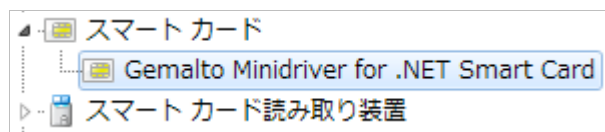
先程 CAB ファイルを展開して生成されたフォルダを指定します。



ドライバのインストールが終了します。



スマートカードとして正常に認識されます。なお、USB-TR はスマートカード読み取り装置として認識されます。



以上で、シンククライアントの設定は終了です。EWF をオンにして再起動します。

3. Gléasでの認証デバイスの準備

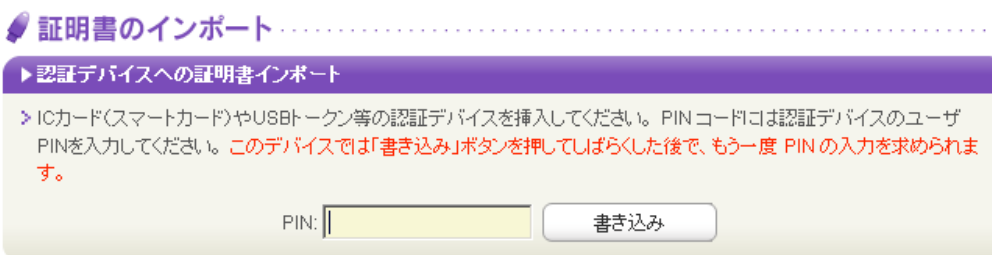
GléasのRAにログインし、スマートカード用に発行した証明書の詳細画面まで移動します。

エンドユーザ用の認証デバイスを管理者端末に接続し、画面上部の[トークンへのインポート]をクリックします。

※事前に認証デバイスのパーソナライズを行っている必要があります。

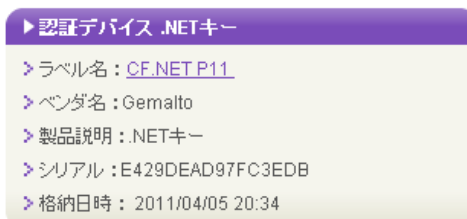


認証デバイスに事前に設定したPIN（暗証番号）を入力し、証明書のインポートを行います。



元の画面に戻ればインポートは成功です。

この時に画面を下にスクロールしていくと、インポート先のデバイス情報が付加されています。



プライベート CA Gléas ホワイトペーパー
WES7 シンクライアントでの XenDesktop スマートカードログオン

また[認証デバイス]メニューでは、この認証デバイスにインポートした証明書を確認することが可能となります。

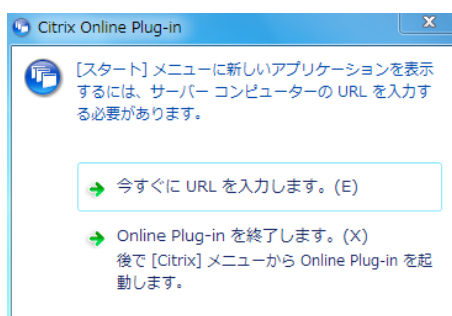


以上で、認証デバイスの準備は終了です。

※Gléasでは、パーソナライズした認証デバイスをエンドユーザに配布し、エンドユーザに証明書のインポートを行わせることも可能です。詳細はJS3までお問い合わせください

4. シンクライアントからのスマートカードログオン

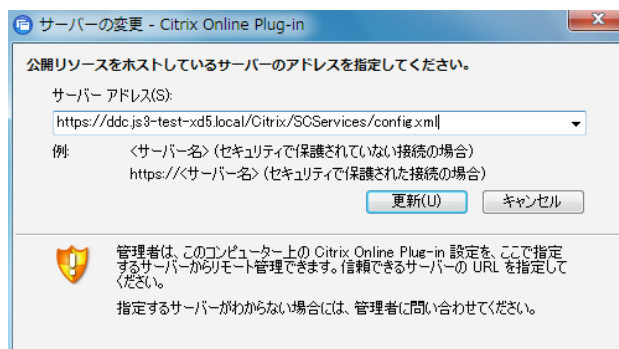
Online Plug-inを起動するとDDCのURLを求めるウィンドウが表示されるので、[今すぐにURLを入力します。(E)]をクリックします。



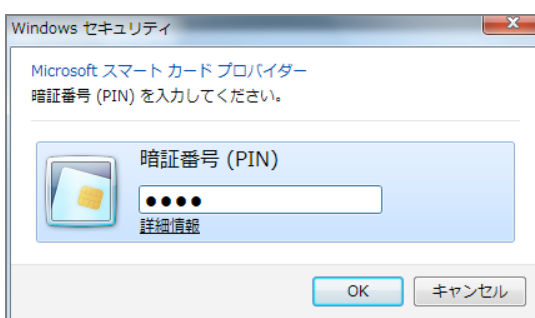
DDCのURLを入力し、[更新(U)]をクリックします。

https:// (ホスト名) / (Serviceサイトのパス) /config.xml

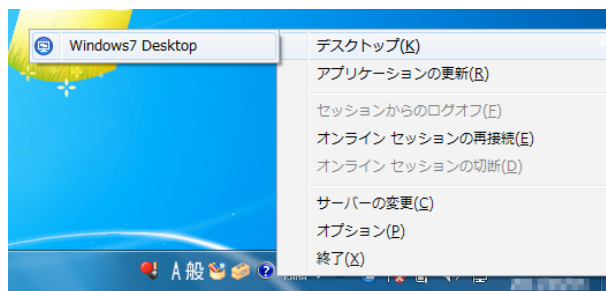
プライベート CA Gléas ホワイトペーパー
WES7 シンクライアントでの XenDesktop スマートカードログオン



認証デバイスのPIN（暗証番号）を求められますので、PINを入力します。



タスクトレイ上のCitrix Online Plug-inアイコンを右クリックし、[デスクトップ]> [(デスクトップ名)]をクリックして、仮想デスクトップにアクセスします。

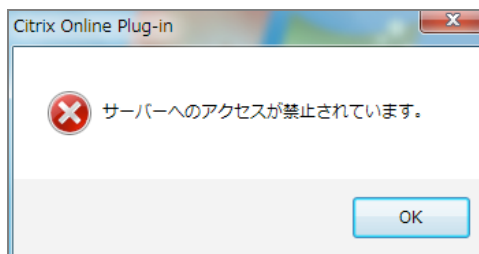


仮想デスクトップ上でスマートカードログオンを行います。再度PINを入力します。



ログオンに成功すると、仮想デスクトップの利用が可能となります。

なお、失効した証明書を格納する認証デバイスを用いて仮想デスクトップにアクセスすると以下メッセージが出現します。



5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■シンクライアントに関するお問い合わせ先

日本ヒューレット・パッカー株式会社
プリンティング&パーソナルシステムズ事業統括
クライアントソリューション本部 製品部

Mail: thinclient.jpn@hp.com

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com