# Cloud Gate SSO Active Directory 設定手順書 (Windows Server2008 R2 Standard Edition)



1.	Active Directory 証明局のインストール	3
2.	証明書の有効期限	23
3.	証明書の作成	25
4.	証明書のエクスポート	30

# 1. Active Directory 証明局のインストール

※既にインストールされている場合はこの手順は不要です。

※Windows Server のインストールディスクが求められる場合があります。

		<ul> <li>▶ リモート デスクトップ サービス</li> <li>◆ iSCSI イニシエーター</li> <li>23 Windows PowerShell Modules</li> <li>◆ Windows Server バックアップ</li> </ul>
コマンド プロンプト メモ帳		<ul> <li>Windows メモリ診断</li> <li>イベント ビューアー</li> <li>コンピューターの管理</li> <li>コンピューターの管理</li> </ul>
Ce Internet Explorer の ペイント ・	Administrator ドキュメント	ユンホーネンド リービス     サーバー マネージャー     ジェ サービス     ジステム構成     ジステム構成     ジステム構成     ジステム     マンド     マン     マン
	コンピューター ネットワーク	<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>
	コントロール パネル デバイスとプリンター	<ul> <li></li></ul>
	管理ツール ・ ヘルプとサポート	3 共有と記憶域の管理
<ul> <li>すべてのプログラム</li> </ul>	ファイル名を指定して実行… 	

スタートメニューから「管理ツール」→「サーバーマネージャー」を起動します。



左ペインから「役割」を選択し、表示された右ペインの「役割の追加」をクリックします。



「次へ」をクリックします。



「Active Directory 証明書サービス」にチェックを付け、「次へ」をクリックします。

役割の追加ウィザード	×			
Active Directory 証明書サービスについて				
開始する前に サーバーの役割 AD CS 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	Active Directory 証明書サービス (AD CS) Active Directory 証明書サービス (AD CS) は、安全なワイヤレス ネットワーク, 仮想プライベート ネットワーク, イン ターネット プロトコル びちいろく (DSe) は、安全なワイヤレス ネットワーク, 仮想プライベート ネットワーク, イン ターネット プロトコル びちいろく (DSe) は、安全なワイヤレス ネットワーク, 仮想プライベート ネットワーク, イン クーネット ログオンなどのシナリオを実現するための証明書基盤を提供します。 <b>注意事項</b> ・ このコンピューターの名前およびドメイン設定は、証明機関 (OA) のインストール後は変更できません。コンピュータ ー名の変更、ドメインの通知、またはこのサーバーのドメイン コントローラーへの昇格を行う場合、CA のインストー ル前にこれらの変更を完了する必要があります。詳細については、「証明機関の名前付け」を参照してください。 <b>ごひけ格組</b> Active Directory 証明書サービスの概要 証明機関の管理 証明機関の名前付け			
	く前へ(P) 次へ(N)> インストール(D) キャンセル			

「次へ」をクリックします。



「証明機関」にチェックを付け、「次へ」をクリックします。

役割の追加ウィザード	×
セットアップの種類の	D指定
開始する前に サーバーの役割 AD CS 役割サービス <del>セットアップの種類</del> CA の種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	<ul> <li>証明機関は、Active Directory のデータを使用して証明書の発行と管理を簡略化できます。エンタープライズ CA とスタンドアロン CA のどちらを使用するかを指定します。</li> <li>エンタープライズ(E) OA がドメインのメンバーであり、ディレクトリ サービスを使用して証明書の発行と管理を行う場合は、このオプションを選択します。</li> <li>スタンドアロン(A) CA がディレクトリ サービス データを使用せずに証明書の発行と管理を行う場合は、このオプションを選択しま す。スタンドアロン CA はドメインのメンバーの場合もあります。</li> </ul>
	エンタープライズ設定とスタンドアロン設定の相違の詳細
	<前へ(P) 次へ(N)> インストール(D) キャンセル

「エンタープライズ」を選択し、「次へ」をクリックします。

役割の追加ウィザード	×
CA の種類の指定	
開始する前に サーバーの役割 AD CS 役割サービス	ルート CA と下位の CA を組み合わせて構成し、階層的な公開キー基盤 (PKD を作成できます。ルート CA と は、その CA 自体が自己署名した証明書を発行する CA です。下位の CA は、他の CA から証明書の発行を受 ける CA です。ルート CA または下位 CA のどちらを設定するかを指定します。 ・ ルート CA(R) 公開キー基盤の最上位の証明機関をインストールする場合、または証明機関を 1 つだけインストールする場合
セット/>>フの種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	(よ、このオフションを選択します。 ● 下位 CA(U) 公開キー基盤の上位にある別の CA から CA 証明書を取得する場合、このオブションを選択します。
	<u> 公開キー基盤 (PKD の詳細</u> <前へ(P) 次へ(N) > インストール(D キャンセル

「ルート CA」を選択し、「次へ」をクリックします。

役割の追加ウィザード	×
秘密キーの設定	
開始する前に サーバーの役割 AD CS 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	<ul> <li>証明書を生成してクライアントに発行するには、CAに秘密キーが必要です。新しい秘密キーを作成するか、既存の 秘密キーを使用するかを指定します。</li> <li>新しい秘密キーを作成する(B) 秘密キーがない場合、または新しい秘密キーを作成してセキュリティを強化する場合は、このオプションを使用します。このオプションを選択すると、暗号化サービス プロバイダーを選択し、秘密キーの長さを指定するよう に求められます。新しい証明書を発行するには、さらにハッシュ アルゴリズムも選択する必要があります。</li> <li>既存の秘密キーを使用する(U) CAの再インストール時に、以前に発行された証明書との連続性を確保する場合は、このオプションを使用します。</li> <li>証明書を超択し、間違付けられている秘密キーを使用する(G) このコンピューターに既存の証明書がある場合、または証明書をインボートしてそれに関連付けられている秘密キーを使用する場合は、このオプションを選択する(E) 以前のインストールがら秘密キーを提択する(E) 以前のインストールがら秘密キーを提択する(E) 以前のインストールがら秘密キーを保持した場合、または代替ソースから秘密キーを使用する場合は、このオプションを選択します。</li> </ul>
	公開キーと秘密キーの詳細
	<前へ(P) 次へ(N)> インストール(1) キャンセル

「新しい秘密キーを作成する」を選択し、「次へ」をクリックします。

役割の追加ウィザード	×
CA の暗号化を構	成
開始する前に サーバーの役割 AD CS 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	新しい秘密キーを作成するには、発行する証明書の用途に合った適切な暗号化サービスプロバイダー、ハッシュ アルコンム、およびキーの長さたたご違択する必要があります。キーの長さに大きな値を遵択すると、セキュリティ は強固になりますが、署名処理に要する時間が長くなります。
	<u>CA の暗号化オプションの詳細</u>
	<前へ(P) 次へ(N)> インストール(1) キャンセル

各設定項目はデフォルトのままで「次へ」をクリックします。

役割の追加ウィザード	×
CA 名を構成	
開始する前に サーバーの役割 AD CS 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 有効期間	この CA を識別する共通名を入力します。この名前は、CA で発行されるすべての証明書に付加されます。識別名 のサフィックスは自動的に生成されますが、変更できます。 この CA の共通名( <u>C</u> ): [testad] 識別名のサフィックス( <u>D</u> ): DC=testad,DC=isr,DC=co,DC=jp ご数別名のブレビュー( <u>V</u> ): CN=testad,DC=testad,DC=isr,DC=co,DC=jp
証明書データベース         確認         進行状況         結果	<u>CA 名の構成の詳細</u>
	<前へ(P) 次へ(N)> インストール(D) キャンセル

「この CA の共通名」に適当な名称を入力して、「次へ」をクリックします。

役割の追加ウィザード	×
証明書データペーン	Aを構成
開始する前に サーバーの役割 AD CS 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 有効期間 証明書データベース 確認 進行状況 結果	証明書データベースは、証明書の要求、発行済み証明書、期限切れ証明書および失効した証明書をすべて記録します。データベースログを使用して、CA の管理アウティビティを監視することができます。         証明書データベースの場所(C):         ○: YWindows¥system32¥CertLog         ● この場所にある、以前のインストールで使用していた証明書データベースを使用する(U):         証明書データベース ログの場所(E):         ○: YWindows¥system32¥CertLog
	<前へ(P) 次へ(N)> インストール(D) キャンセル

「次へ」をクリックします。







「インストール」をクリックします。



「閉じる」をクリックします。



「ファイル名を指定して実行」で「mmc」と入力し、「OK」をクリックします。

<u>  </u>				
🔁 ファイル(F) 操作(A) 表示(V) お気	に入り(O) ウィンドウ(W)	ヘルプ(H)		_ & ×
← 新規作成(N) Ctr	rl+N			
Ctr 上書き保存(S) Ctr	rl+O 名前		操作	
名前を付けて保存(A)		ーに表示する項目はありません。	コンソール ルート	<b>_</b>
スナップインの追加と削除(M) Ctr オプション(P)	rI+M		他の操作	•
1 C¥Wündows¥ ¥ServerManager				
47/A				
- ##21(VV				
, スナップインを追加したり、スナップイン コンソール	, しからスナップインを削除したりで	ごきます。		

ウィンドウが開きますので、「ファイル」→「スナップインの追加と削除」をクリックします。

は、どの拡張を有効にするかを構成 利用できるスナップイン(S): スナップイン ④リモート デスクトップ サービ ①リモート デスクトップ サービ ①リモート デスクトップ セッショ ② ルーティングとリモート アクセ ② ローカル ユーザーとグループ ② 記憶域エクスプローラー ③ 共有フォルダー ③ 承認マネージャー 証明機関 ③ 証明書テンプレート	ベンダー Microsoft Corpor Microsoft Corpor	選択されたスナップイン(E): 「(A) >	<u>拡張の編集(X)…</u> 前除( <u>D</u> ) 上へ移動( <u>D</u> ) 下へ移動( <u>D</u> ) 詳細設定( <u>V</u> )…
。 説明: 「証明機関のプロパティを構成し、こ 」	の CA から発行された証明書を管う	埋することができます。	OK キャンセル

「証明機関」を選択し、「追加」をクリックします。

証明機関	×
このスナップインで管理するコンピューターを選択してください。 - このスナップインで管理するコンピューター ・ ローカル コンピューター(L): (このコンソールを実行しているコンピューター) ・ 別のコンピューター(A): ・ 参照(R)…	
□ コマンド ラインから起動したときは、選択されたコンピューターを変更できるようにする( <u>O</u> ) これは、コンソールを保存した場合にのみ適用されます。	
< 戻る(B) <b>完了 キャンセル ヘルプ</b>	-

「ローカルコンピューター」を選択し、「完了」をクリックします。

スナップインの追加と削除 コンピューターで利用できるスナップ は、どの拡張を有効にするかを構成 利用できるスナップイン(S): スナップイン 通りモート デスクトップ サービ リモート デスクトップ サービ リモート デスクトップ セッショ 夏ルーティングとリモート アクセ シローカル ユーザーとグループ 記憶域エクスプローラー 愛共有した記憶域の管理 愛共有フォルダー 読録マネージャー 読明書 一記明書 一記明書	インからこのコンソールに想 気できます。 Microsoft Corpor Microsoft Corpor	使用するスナップインを <u> </u>	選択したり、選択したスナップインを構成 選択されたスナップイン(E): コンソール ルート 注意証明機関(ローカル)	★ はたりできます。拡張可能なスナップインで 拡張の編集(½)… 前序余(R) 上へ移動(U) 下へ移動(D)
説明:  証明書スナップインを使うとユーザ・ 	-、サービス、またはコンピ:	ューターの証明書スト	アの内容を表示できます。	OK キャンセル

「証明書」を選択し、「追加」をクリックします。

証明書スナ <del>ッ</del> プイン	×
このスナップインで管理する証明書:	
○ ユーサー アカワンド(M) ○ サービス アカウンド(S)	
	< 戻る(B) 次へ(N) > キャンセル

「コンピューターアカウント」を選択し、「次へ」をクリックします。

コンピューターの選択	×
このスナップインで管理するコンピューターを選択してください。 このスナップインで管理するコンピューター: ・ ローカル コンピューター(L): (このコンソールを実行しているコンピューター)) ・ 別のコンピューター(A): 参照(B)	
□ コマンド ラインから起動したときは選択されたコンピューターを変更できるようにする( <u>W</u> ) これは、コンソールを保存した場合にのみ適用されます。	
< 戻る(B) 完了 キャンセル	]

「ローカルコンピューター」を選択し、「完了」をクリックします。

<ul> <li>マリカビマるスノックイノ(3):</li> <li>スナップイン</li> <li>リモート デスクトップ</li> <li>リモート デスクトップ サービ…</li> <li>リモート デスクトップ セッショ…</li> <li>ルーティングとリモート アクセ…</li> <li>ローカル ユーザーとグループ</li> <li>記憶域エクスプローラー</li> <li>民情域エクスプローラー</li> <li>民情域の管理</li> <li>共有フォルダー</li> <li>課題明機関</li> <li>第回目書</li> </ul>	ベンダー Microsoft Corpor Microsoft Corpor	2017年1月1日日 2017年1月1日 2017年1月11日 2017年1月11日 2017年1月11日 2017年1月11日 2017年1月11日 2	<u>拡張の編集(2)…</u>
図 <u>記の月書テンプレート</u> 説明: 証明書のテンプレート スナップイン	Microsoft Corpor	よび管理を行うことができます。	詳希語設定(⊻)

「証明書テンプレート」を選択し、「追加」をクリックします。



「OK」をクリックします。

#### 2. 証明書の有効期限

コンソール1 - 「コンソール ルート¥証明書テンプレート」	(WIN-A0535G7VQQN.testad.isr.co.jp	o)]		
🚟 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィ	ンドウ(W) ヘルプ(H)			_ 8 ×
♦ ♦ 2 00 00 00 00 00 00 00 00 00 00 00 00 0				
□ コンソール ルート	テンプレート表示名 ・	最小限サポートされている	操作	
🗉 📷 証明機関 (ローカル)	🖳 CA Exchange	Windows Server 2003 E		
🖃 🔂 証明書 (ローカル コンピューター)	🖳 CEP 暗号化	Windows 2000	計明者) ノノレート (#IN-A0333G/V	aan.tes 🔺
🗵 証明書テンプレート (WIN-A0535G7VQQN.testad.is	🗟 EFS 回復エージェント	Windows 2000	他の操作	•
	回 Exchange ユーザー	Windows 2000		
	回 Exchange 署名のみ	Windows 2000	下メイノコノトローフーの認証	<u>^</u>
	回 Exchange 登録エージェント (オフライン専	要求) Windows 2000	他の操作	•
	🖳 IPSec	Windows 2000		
	🖳 IPSec (オフライン要求)	Windows 2000		
	🖳 Kerberos 🔝	Windows Server 2003 E		
	🖳 OCSP 応答の署名	Windows Server 2008 E		
	🖳 RAS および IAS サーバー	Windows Server 2003 E		
		Windows 2000		
	▲ キー回復エージェント	Windows Server 2003 E		
	凰 クロス証明機関	Windows Server 2003 E		
		Windows 2000		
		Windows 2000		
		Windows 2000		
	圏 スマート カード ロクオン	Windows 2000		
		Windows Server 2003 E		
		Windows 2000		
		テンプレートの複製(U)		
		正明書保持者をすべて再登録する(E)		
	国 ユニリニオロのの	‡ለፕፖመタスク(K)	•	
	風 ワークステーション認証	プロパティ(R)		
	風下位の証明機関	(ルプ(H))		
	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	Windows 2000		
	圆 基本 EFS	Windows 2000		
	🗟 信頼リストの署名	Windows 2000		
	😡 登録エージェント	Windows 2000		
	回 登録エージェント (コンピューター)	Windows 2000		
	😡 認証されたセッション	Windows 2000		
4	4	Þ		
選択した項目のプロパティ ダイアログ ボックスを開きます。		· · · · · · · · · · · · · · · · · · ·	, 	

「証明書テンプレート」をクリックし、「ドメインコントローラの認証」で右クリックして、「プロパティ」を選択します。

ドメイン コントローラーの認証のプロパティ ? 🗙
優先するテンプレート 拡張 レセキュリティ サーバー 全般 要求処理 サブジェクト名 発行の要件
テンプレート表示名(E):
」ドメインコントローラーの記録正 最小限サポートされている
CA: Windows Server 2003 Enterprise
DomainControllerAuthentication
右如期間(\A) 再新期間(B)
<ul> <li>Active Directory の証明書を発行する(P)</li> <li>Active Directory (ご重複する証明書がある場合、自動的に再登録しない(D)</li> </ul>
□ スマートカード証明書の自動更新で、新しいキーを作成できない場合は既存の □ キーを使用する(F)
OK キャンセル 適用( <u>A</u> ) ヘルプ

「有効期限」を確認し、20年などの長い期間に設定し、「OK」をクリックします。

本設定を行なっても、期間が証明書に反 映されない場合があることを確認出来 ております。 その場合は、構築ベンダー様にご確認頂 くか、デフォルトの期間のままで発行を お願いいたします。

#### 3. 証明書の作成



mmc の左ペインで「証明書」→「個人」→「証明書」を選択します。

中央ペインの何もないところで右クリックし、「すべてのタスク」→「新しい証明書の要求」をクリックします。

■ 証明書の登録
📮 証明書の登録
開始する前に
次の手順では証明書をインストールします。証明書はデジタル資格情報で、ワイヤレス ネットワークへの接続、コンテンツの 保護、識別情報の確立、およびその他のセキュリティ関連タスクの実行に使用されます。
証明書を要求する前に、次の点を確認してください。
使用するコンピューターがネットワークに接続されている 証明書を取得する権利があることの確認に使用できる資格情報を持っている
<u>デジタル語単月書の語語細</u> を表示します
次へ(N) キャンセル

「次へ」をクリックします。

■証明書の登録	IX
🗊 証明書の登録	
<b>証明書の登録ポリシーの選択</b> 証明書の登録ポリシーは、あらかじめ定義された証明書テンプレートに基づく登録を可能にするものです。場合によっては、 証明書の登録ポリシーは既に構成されていることがあります。	
システム管理者が構成します	1
Active Directory 登録ポリシー	
コーザーが構成します 新規追加	
次へ(N) キャンセル	

「Active Directory 登録ポリシー」を選択し、「次へ」をクリックします。

ー 種類の証明書を要求できます。要求する証明 Active Directory 啓録ポリシノー	月書を選択し、「登録] をクリックしてください。	
ロディレクトリ電子メール レプリケーション	• 状態:利用可能	言羊糸田
ד אלט בטאם איי	(1) 状態:利用可能	言羊糸田
☞ ドメイン コントローラーの認証	(i) 状態:利用可能	言羊糸田
」 すべてのテンプレートの表示( <u>A</u> ) 19日表 ☆美谷(mt まニ」 まま		

「ドメインコントローラの認証」を選択し、「登録」をクリックします。

📭 証明書の登録		
📪 証明書の登録		
証明まインストールの結果		
	- 1	
次の証明書が登録され、コンピューターにインス	くトールされました。	
Active Directory 登録ポリシ	/-	
☞ ドメイン コントローラーの認証	✓ 状態: 成功	≣¥約田 ⑧
		完了(F)

「完了」をクリックします。

## 4. 証明書のエクスポート



中央ペインで今作成したエクスポートする証明書を選択し、右クリックで表示されるメニューから、 「すべてのタスク」→「エクスポート」を選択します。



「次へ」をクリックします。

密キーのエクスボート	
秘密キーを証明書と一緒にエクスポートすることが	できます。
秘密キーはパスワードで保護されています。秘密 を入力する必要があります。	キーを証明書と一緒にエクスポートする場合は、パスワー
証明書と一緒に秘密キーをエクスポートしますか?	,
○ はい、秘密キーをエクスポートします(Y)	
● いいえ、秘密キーをエクスポートしません(	(O)
注意: 関連付けられた秘密キーにはエクスポート? できます。	不可能フラグが付いています。証明書だけをエクスポート
注意: 関連付けられた秘密キーにはエクスポート <sup>2</sup> できます。	○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○
注意: 関連付けられた秘密キーにはエクスポート <sup>2</sup> できます。 <u>*キーのエクスポートの詳細を表示します</u>	○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○

「いいえ、秘密キーをエクスポートしません」がチェックされていることを確認し、「次へ」をクリックします。

使	用する形式を選択してください。
	C DER encoded binary X.509 (.CER)( <u>D</u> )
	Base 64 encoded X.509 (CER)(S)
	○ Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B)( <u>C</u> )
	▶ 証明のパスにある証明書を可能であればすべて含む(1)
	C Personal Information Exchange - PKCS #12 (.PFX)( <u>P</u> )
	▶ ■ 証明のパスにある証明書を可能であればすべて含む(以)
	▶ 正しくエクスポートされたときは秘密キーを削除する(火)
	すべての拡張プロパティをエクスポートする(A)
	C Microsoft シリアル化された評明書ストア (SST)(T)

「Base64 encoded X.509(CER)」を選択し、「次へ」をクリックします。

証明書のエクスボート ウィザード	×
エクスポートするファイル	
エクスポートするファイルの名前を入力してください	
ファイル-名(F)・	
C:¥Users¥Administrator¥Desktop¥testcert.cer	参照(民)
	< 戻る(B) 次へ(N) キャンセル

「ファイル名」を入力し、「次へ」をクリックします。 ※ファイル名はなんでも構いません。

証明書のエクスポート ウィザード		×
	証明書のエクスポート ウィザート	の完了
	証明書のエクスポート ウィザードが正常に完了しました。 次の設定が指定されました:	
	ファイル名 キーのエクスポート 証明のパスにあるすべての証明書を含める ファイルの形式	C¥Users¥Administr いいえ いいえ Base 64 Encoded X
	< 戻る( <u>B</u> ) 5	完了 キャンセル

#### 「完了」をクリックします。

証明書のエクスポート ウィザード	X
正しくエクスポートされました。	
(ОК	

「OK」をクリックします。

## 参考:証明書の内容

🐌 test.cer - Jモ帳	
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルプ(H)	
BEGIN CERTIFICATE	<b>_</b>
MIIFR;CCBC6gAwIBAgIKGISp/wAAAAAAAAAAkkabkahkiG9w0BAQUFADA7MRUwEwYK	
CZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgR0ZXN0MQwwCgYDVQQD	
EwNpc3IwHhcNMDkwMTMwMDIyMDI4WhcNMTEwMTMwMDIzMDI4WjAAMIGfMA0GCSqG	
SIb3DQEBAQUAA4GNADCBiQKBgQCYKBP+Ah1cRwfIJyWhANWdmV3FafU0v6/OUhrm	
j0Qy48M4Ed+dW02oghYWSJLAUyDU7Ja4epQo92o/QgVNNJ3L6I7GXv2Ny6CkFeQ7	
/EFzF+tvwRFF2ua+4MU3Z987i4z4xQpPDFf1nFv4p0/6nE2xqTJ1vQ8p0YiXhxcb	
fxXXiwIDAQABo4IDCTCCAwUwCwYDVR0PBAQDAgWgMB0GA1UdDgQWBBScf4GR1HSj	
EyJ/0SKacHEPH5MWxTA3BgkrBgEEAYI3FQcEKjAoBiArBgEEAYI3FQiBzP8whfic	
MISInzCFr/xKhYyNCE0BHAIBbgIBATAfBgNVHSMEGDAWgBRFZ2myksUKSbEfoNbR	
/WOnEIxBczCB8AYDVR0tBIHoMIHIMIHioIHtoIHchoGqbGRhcDovLy9DTj1pc3Is	
Q049dGVzdGFkMDEsQ049Q0RQLENOPVB1YmxpYyUyMEtTeSUyMFN1cnZpY2VzLENO	
PVNTcnZpY2VzLENUPUNvbmZpZ3VyYXRpb24sREM9dGVzdUxEUzTsb2NhbU9jZXJU	
aWZpY2FUZVJIdm9jYXKpb25MaXNUP2Jhc2U/b2JqZWNUU2xhc3M9YIJMKGIzdHJp	
TNVUaW9uUG9pbnSGLWhUdHA6Ly9UZXNUYWUwMS5UZXNULmxvYZFsLUNTcnKFbnJv	
DGWVAXNYLMNYDDUCAUMGUUSGAUUFBWEBBIHZMIHZMIGhBggrBgEFBUCWAOaBIGXK	
YAADEYXVQU49aANYLENUPUFJQ5xD1	
J     ZAJZANNI CYXU   J   UDZOMANGI CMEVANGULEKUPAKI COUSKEMODOUJ I NYW TUEU   ZY 10 - MIZ- YOE0 ZTO : YYNU DOO :YY: JENI-YYNI-DMNUD- ZI : YYD-LOEDJYD-LO LO	
ZAJUAYYZPTZEUZTUTI Y TANTEZU TAMI EZU TAMU JI CENSTANZEYYN I CORPZMI U TARPOZUDCIARODU UP L-IULIU TOY TIZU YDDOL UDALZONIID AUTACLIU OCZYNIOZNIO MOSO ZYNIOLIWU WYDDOL	
ankwiwiwiiikwibbwoniiikakawiinoanaolyyyuzanoimiwiwiiisyuzanolnixyizesloniichke  bolude:uude://=deel/MDEude://=de5ob2NbbE9ob27.000//22.000/22.000/23.001/00:Me4eeeoc	
IDHOVDAWVAAVZAALKIMDEAAAVZACOSDZNEDEOPCOTATOOOMOKAATOAOGAATIMAAACOSA IAAHIERuuMARaareRaEERA-DAAVVIVUVVRRACANVAAATATOAOMOKAATOAOGATIMAAACOSA	
Incordanterumedesetdsetdsetdsetaattervetddadenxaeatattartbeetaatterumedesetdsetaatterumedesetdsetaatterumedese	
EVITAGVZAGELMDEUAGVZAC5ab2NbbDANRølzable; G9w0RAOUEAAOCAOEAM+KbMuDa	
ib107bzwTIstXi77a04r00crM90ePWGvbo.ISG//IWX7mNBSGVc.IkHpiSNEkv8UDLb	
w7UcLCBY+8.JvLivafbWcWzGc94gSNFG3v8f770S4+i76VVTbuvmWB8CK109iUrY0	
roaC6LSdktaiuX8vER0b0mw15ax9iACEbfzub3VvXXwCT.1/aSP/+fNb5W9.1uk4Ve	
mEv7k7EHRix+Dn7YEAxCrw9uYKXr7h1XJvKp2s1WokV5Psw7pRPSwAXvE0iQ1sLW	
L69Ym/sRLzYJF6Xv52o8SWTghge1aA6DSQU07Bg8vvVI/epUdmed8609xtY0TTCU	
DbzV0baMf/14sg==	
END CERTIFICATE	
	► //