ID.logon Key-Manager

Kurzbeschreibung

Version 1.0

Inhaltsverzeichnis

1 Beschreibung

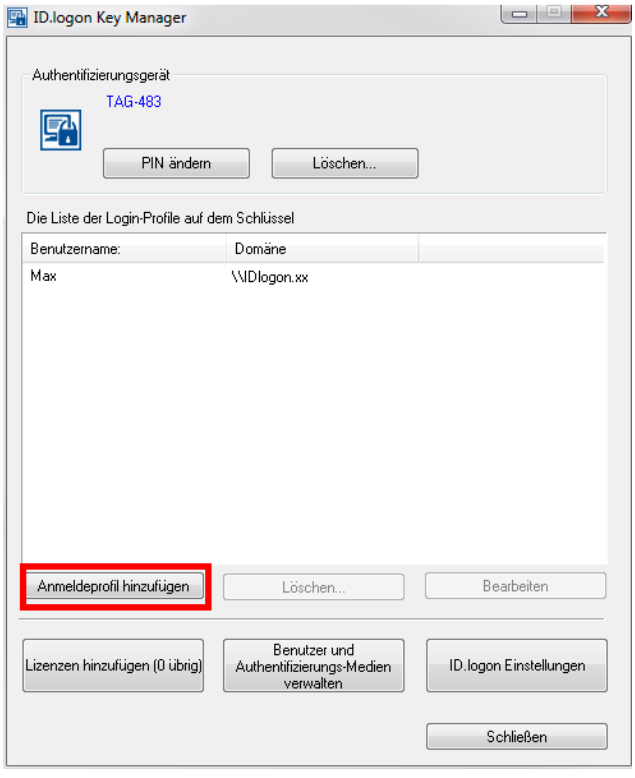
Mit dem ID.logon Key-Manager können Sie 2-Faktor-Authentifizierungsschlüssel von einer zentralen Stelle aus erstellen und verwalten.

Der Einsatz des Key-Managers empfiehlt sich, wenn die Anzahl an Benutzern und Arbeitsstationen einen gewissen Umfang erreicht hat. Somit sparen Sie Zeit bei der Erfassung und Verwaltung der RFID Medien bzw. Authentisierungs-Schlüssel und müssen nicht jedes einzelne Profil an jeder einzelnen Arbeitsstation anmelden.

2 Funktionen:

2.1 Anmeldeprofile

Mit dem Key-Manager können Sie zentral alle Anmeldeprofile anlegen. Dazu sind Admin-Rechte erforderlich. Bei der Ersterfassung der Profile benötigen Sie noch User-ID und Passwort des jeweiligen Benutzers.



2.2 Authentisierungs-Schlüssel

Beim Anlegen von Anmeldeprofilen werden Authentisierungs-Schlüssel gespeichert. Diese gelten für alle Arbeitsstationen, auf denen die ID.logon Anwendung installiert ist. Der Schlüssel beinhaltet die Windows-Credentials User-ID und Passwort. Dies sind AES 256 Bit verschlüsselte XML-Dateien und damit unter heutigen Sicherheitsgesichtspunkten nicht oder so gut wie nicht reproduzierbar.

2.3 PIN-Code-Sicherheit

Ein PIN-Code kann zusätzlich zum Schutz des RFID Mediums über den Key-Manager jederzeit eingerichtet und auch wieder deaktiviert werden.

Falls das Authentifizierungs-Medium nach drei erfolglosen PIN-Versuchen gesperrt wurde, kann dies von einem Administrator über den Key-Manager entsperrt werden.

2.4 Roaming-Anmeldeprofile.

Erstellen und verwenden Sie Roaming-Anmeldeprofile auf einem Authentifizierungsschlüssel, mit denen Sie sich an jeder beliebigen Arbeitsstation anmelden können.

2.5 Installation und Betrieb

Der Key-Manager kann auf jeder x-beliebigen Arbeitsstation im Netzwerk installiert und betrieben werden. Jeder Key-Manager muss einzeln über einen Lizenz-Code lizensiert werden. Ein Lizenz-Code ist im Lieferumfang der Software enthalten.

2.6 Shared Folder

Für die gemeinsame Verwaltung der Anmeldeprofile über den Key-Manager wird ein Shared-Folder im Netzwerk angelegt. Dieser muss über Schreib-Leserechte für jeden Benutzer verfügen. In diesem Ordner sind dann alle Authentisierungs-Schlüssel für alle Benutzer abgelegt.

2.7 Speicherung von Key-Files im Active-Directory

Wenn die Ablage der Schlüssel in einem Shared-Folder nicht gewünscht ist, besteht die Möglichkeit, im Active Directory eine separate Tabelle anzulegen. Dort werden dann die Schlüssel abgelegt und sind somit gegen Löschen und Kopieren gesichert. Dazu bedarf es einer weiteren Ausbaustufe des Key-Managers.

Die Installation der Tabelle auf dem AD erfordert weitreichende Rechte und einen einmaligen Installationsvorgang auf dem Domain-Controller. Hierzu sind dann im Vorfeld Abläufe und die Vorgehensweise mit der IT zu besprechen. Dies erfordert ein zusätzliches Kontingent an Dienstleistungs-Aufwand.