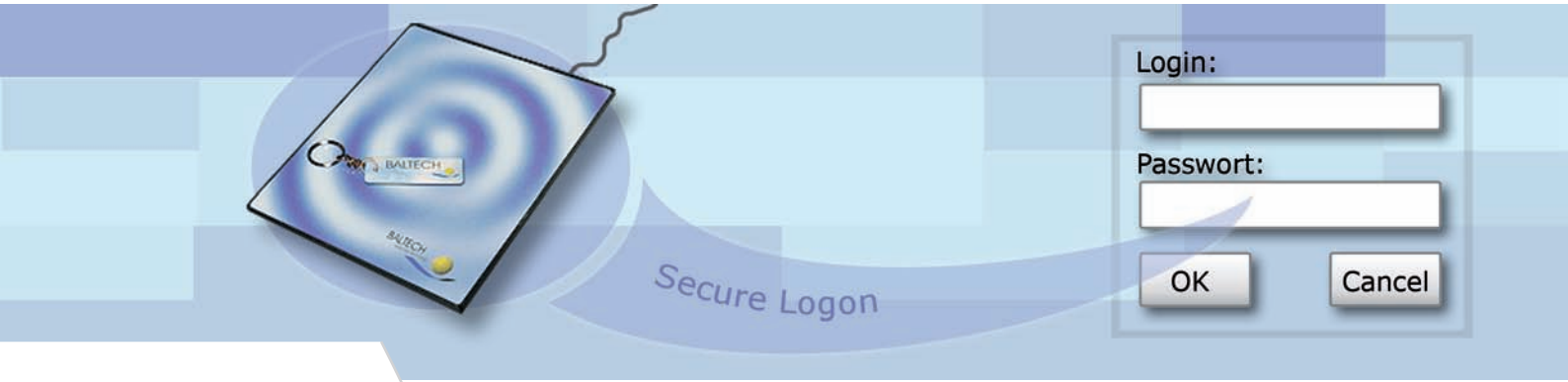


Internetnutzung an öffentlich zugänglichen Internetterminals

mit RFID-Mitarbeiterausweisen

Es soll einem eingeschränkten Benutzerkreis in Universitäten, Krankenhäusern, Verkaufseinrichtungen und an vielen anderen Orten ermöglicht werden, öffentlich zugängliche Internetterminals zur freien Nutzung zur Verfügung zu stellen.

Herausforderung

Bereits im Einsatz befindliche kontaktlose Hausausweise, Zugangskarten bzw. leihweise ausgegebene Gästekarten sollen die Freischaltung der Internetterminals komfortabel ermöglichen.
Darüber hinaus soll im Fall des Missbrauchs des Internetzugangs für kriminelle Handlungen ermittelbar sein, welche Servicekarte in den jeweils betreffenden Zeiträumen für die Freischaltung des Internets benutzt worden ist.

Da die Internetterminals kontinuierlich laufen erfolgt die Anmeldung an Windows automatisch per Autologon. Die Login-Informationen liegen im geschützten Bereich der LSA (Local Security Authority). Das Internetterminal läuft sofort nach dem Hochfahren in den gesperrten Modus und kann nur unter Eingabe des im LSA abgelegten Passwortes freigeschaltet werden. Man müsste Nutzern des Terminals das gleiche Passwort zur Verfügung stellen, wobei nicht mehr nachvollziehbar wäre, welcher Nutzer wann das Terminal benutzt hat.
Auditierungen fordern hingegen die zweifelsfreie Nachweisführung der Nutzung öffentlicher Internetterminals. Wünschenswert ist, dass die Anmeldeinformation zukünftig nicht mehr preisgegeben werden muss und dennoch eine aufwändige Nutzerverwaltung entbehrlich ist.

Quelle: Werkstation GmbH

Lösung

Windows Autologon führt zur sofortigen Sperrung des Systems, die Entsperrung des PC erfolgt mit dem Einsatz kontaktloser Servicekarten. Über Sicherheitsgruppen erhält ein bestimmter Personenkreis die Berechtigung zum Entsperren der Arbeitsstation.

Alle ausgeführten Aktionen werden in einer internen Datenbank protokolliert und dienen der Nachvollziehbarkeit des Anmeldeprozesses anhand der UID des Betriebsausweises. Eine USB-Blocker-Software stellt sicher, dass nur RFID-Leser mit einer eingestellten Seriennummer am USB-Port betrieben werden können.

Umsetzung

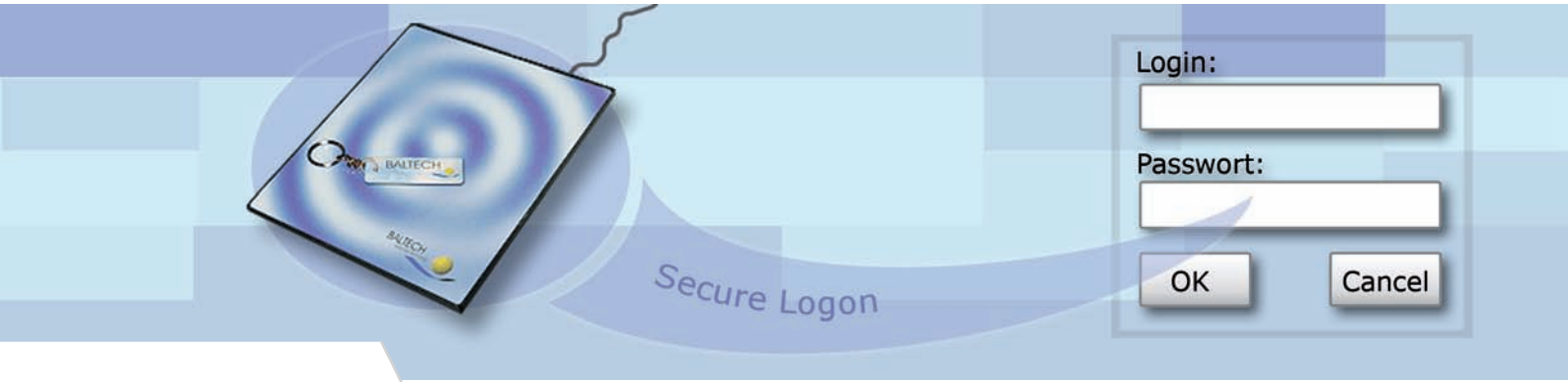
Auf dem PC-Terminal wird digitronic Secure Logon installiert, dies ermöglicht die Anmeldung an PC Arbeitsplätzen bzw. mobilen Geräten mit verschiedensten bereits im Einsatz befindlichen Karten (z.B. Mitarbeiterausweisen).
Die Erkennung des RFID-Ausweises erfolgt über einen Baltech-Leser. Dieser fragt die eindeutige UID des Ausweises ab und ordnet sie einer Sicherheitsgruppe zu. Es wird geprüft, ob die ermittelte UID Mitglied der berechtigten Sicherheitsgruppe ist und gegebenenfalls wird das Interneterminal entsperrt.
Die Protokollierung der Aktionen erfolgt mit Hilfe des digitronic Token Management Systems. Es wird nachvollziehbar, welche Servicekarte zu welchem Zeitpunkt den PC entsperrt hat. Der Einsatz des digitronic Universal Device Blockers (UDB) stellt sicher, dass nur Geräte mit bestimmten Seriennummern am USB-Bus zugelassen werden (z.B. RFID-Leser).

digitronic secure

digitronic
computersysteme gmbh
Oberfrohnaer Str.62
09117 Chemnitz

Telefon +49 (0) 371 81539-0
Fax +49 (0) 371 81539-900

info@digitronic.net
www.digitronic.net



Wir stellen uns vor

Mit der digitronic computersysteme gmbh sicher in die Zukunft …

Die digitronic computersysteme gmbh ist ein führender Hersteller und Lieferant von Kommunikations- und Datensicherheitslösungen, welche es nicht nur Unternehmen jeglicher Größe, sondern auch Endanwendern ermöglicht, innovativ zu kommunizieren und elektronische Daten vor Datenmissbrauch zu schützen. Aufgrund umfassender Service- und Beratungsdienstleistungen zeichnet sich digitronic durch Kundennähe, kurze Projektumsetzungszeiten und höchste Servicequalität aus.

Fakten und Highlights

Die digitronic computersysteme gmbh wurde 1991 in Chemnitz gegründet und entwickelte in enger Kooperation mit der Polizei mehrerer Bundesländer das vorschriftenkonforme Unified Messaging System WinTelex EP. Kernkompetenzen im Bereich automatischer Kommunikationssysteme führten zu höchster Nutzerakzeptanz verbunden mit modernsten Übertragungstechnologien.

Parallel dazu entwickelte digitronic Sicherheitssoftware, die unter dem Produktnamen digitronic Security Suite erfolgreich vermarktet wird. Kernphilosophie des Produktes ist die Erhöhung der Sicherheit bei steigendem Komfort. Dies wird ermöglicht durch den Einsatz verschiedenster Authentifizierungsmittel (Smartcards, RFID-Token etc.) über standardisierte Schnittstellen.

Im Jahre 2005 wurde die Authention Safety Suite durch die Verschlüsselungssoftware Crypted Group Share erweitert. Crypted Group Share bietet Managern, Personal- und Entwicklungsleitern sichere Datenräumen in IT-Infrastrukturen in Form von Abteilungs- und Datentresoren. Der wirksame Ausschluss administrativer Einblicke und die dennoch komfortable Teamarbeit mit Vertrauenspersonen überzeugen durch plausible Einfachheit.

2007 stellte digitronic mit der polizeilichen KommunikationsBox (pKommBox) die erste Formelle Endstelle, der Deutschen Polizei mit Outlook-Integration, vor. Ein von digitronic speziell dafür entwickeltes AddIn bietet dem Anwender ein Formular zur Erstellung und Anzeige formeller Nachrichten.

Aufbauend auf der siebenjährigen Crypted Group Share -Produkterfahrung erfolgt im Jahr 2012 die Markteinführung von HiCrypt als digitaler Tresor mit Schlüssel-Alleinbesitzgarantie.

digitronic secure

digitronic
computersysteme gmbh
Oberfrohnaer Str.62
09117 Chemnitz

Telefon +49 (0) 371 81539-0
Fax +49 (0) 371 81539-900

info@digitronic.net
www.digitronic.net