



CREDENTIAL MANAGEMENT SYSTEM

**The enterprise solution
that provides complete
credential management with
state-of-the-art security**

Authentication and security solutions you can trust.™

AUTHENTX™ Credential Management System

CMS is the comprehensive enterprise solution to manage and maintain credentials and access control in a secure, error-free environment that is easy to use. No other solution provides the depth of services and control of CMS. Its features include credential management and revocation including ID data collection, photographic, signature and biometric template capture, card/ID token issuance and encoding, token and identity authentication, visitor enrollment and control, global LDAP database services, and universal device connection using the socket API.

CMS provides a well-designed user interface that facilitates the capture and storage of credential and personal information data. The system provides for data field entry, photograph capture, biometric fingerprint scan, and signature image capture. Data can be stored locally on an SQL compliant database or across a LAN connection to an LDAP compliant server, making data export both simple and secure.

The system can be customized to meet a wide variety of needs.

A SYSTEM FOR THE NEW REALITY

Today, more than ever, enterprises face the challenge of providing security to their facilities and networks, whether for dozens or thousands of credential holders. This security must be provided in a technological environment where almost anyone can have access to tools that allow for creation and duplication of credentials.

The CMS is the only commercially available smart card management system that complies with the most stringent Federal Government standards. Built on the core AuthentX™ Authentication Server, CMS is a complete card issuance, token authentication and credential management solution that provides full card personalization, card production, flexible card design, access control, and application interface to various legacy systems. It is a complete web browser-based server solution that is scalable from one to 100 million credentials.

Configurable with modular components, AuthentX™ CMS, in conjunction with web browsers on the workstation, captures data, photographs and biometrics, enrolls credentials, manages data, provides revocation services, and interfaces with almost any token credential-based application. The system also provides the ability to track ID expiration, application and container management, revocation history, smart card activation and deactivation, credential holder privileges, lost and stolen cards tracking, lost cards regeneration, card number management, and basic and ad hoc report generation.

The system transmits encrypted data securely (using Secure Sockets Layers, or SSL) through Windows® 2000 or higher operating systems and is fully accessible through Microsoft® Internet Explorer (versions 5.0 and higher) thus ensuring ease-of-use and minimal training expenses.

CUTTING-EDGE DATABASE TECHNOLOGY

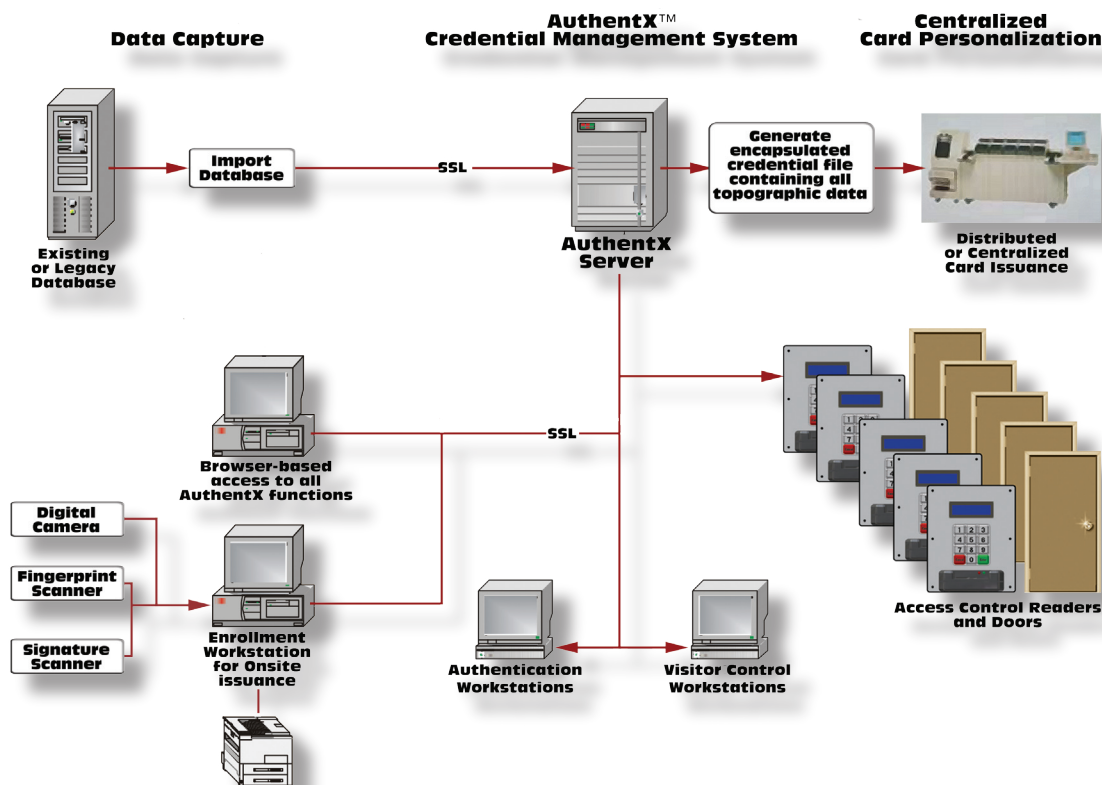
The unique design of the AuthentX™ CMS provides the user a choice in database implementation: centralized or decentralized, positive or negative, hosted or in-house. The credential data needed to authenticate the card or individual can be stored exclusively on the AuthentX™ Authentication Server or distributed to the authentication devices.

The AuthentX™ System allows network connectivity in SQL, ODBC, XML, or any standard access mode, over TCP/IP. The preferred method, however, is to utilize the LDAP (Lightweight

Directory Access Protocol) with a back-end database. LDAP allows all databases in the online system to be self-replicating through a set of predefined rules. The LDAP server provides a ready way of maintaining redundant data across the enterprise.

Utilizing LDAP architecture and its innovative online/offline revocation capability, the AuthentX™ Authentication Server hosts the database and applications for credential management. It allows the authorized users to access the LDAP database, using their Internet browser and perform necessary card management functions.

CMS creates self-synchronizing databases to ensure all of them have identical information and allows logical and physical access systems to coordinate information without actually allowing sessions across the networks.



The end result: security is not compromised. Logical and physical access networks remain separate. Not only can legacy databases be bridged with the LDAP so all new applications are communicating with the LDAP in a standard manner, the LDAP can negotiate with a legacy system on the back-end.

Keep your legacy applications: interoperability fully achieved.

STATE-OF-THE-ART AUTHENTICATION

CMS was developed to meet or exceed the most stringent government standards. For over a decade XTec has been a leader in the development of the standards used by the Federal Government to establish error-free and secure authentication. It verifies cardholder identity with the triad of authentication factors:

- Something the person has** – a secure card or token,
- Something the person knows** – a PIN, or some other code, and
- Something the person is** – a photographic or fingerprint biometric.

CMS utilizes smart cards, personal identification numbers (PINs), and photographic or fingerprint biometric templates for personal identity authentication. It captures and stores digital photographs at 300 dpi or higher, fingerprint biometrics template and data. Card authentication using cryptographic challenge / response is an integral part of CMS. During issuance, each card can be injected with a unique secret key, derived from selected data stored in the card and a seed key securely maintained by the card issuer. It is this secret key on the card that provides proof of authenticity. All XTec readers and authentication devices used in the CMS have

built-in capability to support many other card authentication methods.

Utilizing state-of-the-art card authentication methods each credential can be positively confirmed and together with authentication of the data it ensures that the biometric templates stored on the credential can be trusted.

The CMS can completely authenticate the card and the identity of the cardholder—at any viewing station.

WIRELESS TECHNOLOGY

One of the most innovative features of CMS is its ability to utilize cutting-edge technologies to maintain security and data integrity. Revocation of credentials, for example, can be implemented in a wired online environment, as well as offline through the use of a national wireless paging system. The user can initiate an encrypted revocation transaction, send it through the paging service, and immediately update revocation lists in all readers and viewing stations equipped with wireless receivers.

Revocation lists are set up on the AuthentX™ Authentication Server, in the local database, and in the readers, as an exception list. This list is always referred to before privilege is granted.

The Remote Viewing/Verification Stations provide real-time verification and authentication of the credential without the need to be on-line.

VISITOR CONTROL SYSTEM MODULE

The Visitor Control System is an optional module of CMS that can be fully integrated into the final CMS installation. It was originally developed by XTec to meet the stringent security requirements of the United States Department of State. It is a comprehensive solution that supports online and offline operation, photo/image capture, activity tracking, interfaces to access control systems, advance enrollment via secure web page, authentication using media from drivers' license, and visitor badge generation. It also includes an extensive set of report and forensic search capabilities. It is capable of maintaining a forensic database, for biometric reasons.

In its standalone version, the Visitor Control System conveniently captures visitor information and stores it locally while printing a temporary visitor badge. It features a self-contained visitor access database, report generator, transaction log and historical archive manager. The workstation can be configured as a kiosk or as a PC on a tabletop or desk.

When integrated within CMS, the Visitor Control System will support other visitor control modules tied to one or multiple servers across large geographical areas, and can interface with numerous access control systems for a complete solution.

In either form, the visitor control system is fully capable of time-stamping and storing visitor access information, exporting and downloading information to a reporting system, and generating visitor reports.

REPORT WRITING

Reports can be sent to standard printers that support images and data. Third-party report generators, such as Crystal Reports, or other similar report writers, can be used to generate a significant number of customized reports.

CONTACT US

XTec is a world-leader in authentication systems and access control. Call us to discuss how your company can benefit from the security provided by AuthentX™ CMS and other XTec products.

CMS provides a full set of card issuance, tracking, and revocation services with the following features:

Photo ID Subsystem

- Token topology design for printing
- Create multiple token print templates
- Image capture with quality adjustment and automatic image positioning and image cropping
- Incorporate image files
- Incorporate data variables (data from DB)
- 1D and 2D bar codes
- Micro printing / security feature
- Printer interface

Card/ID Token Issuance Subsystem

- Web/Browser based interface
- Customizable data content and collection fields
- Customizable business rules for auto-fill data items
- Administrative override for auto-fill data items
- Pick-list data items with maintenance capability
- Secure Authentication Key injection systems
- Card vendor independent with auto-detection
- Multi-medium encoding (magnetic, contact, contactless)
- Plug-ins for new cards and card-types
- Full-featured credential issuance system (all medium)

Credential Management and Revocation Subsystem

- Global LDAP database services
- X-Schema (Credential, Identity, Permissions)
- Encrypted data transfer and storage
- Activity logging and history tracking
- Scalable from one to 100 million credentials
- Web based (browser) interface
- Segmented domain access control
- Online/offline use
- Networked and/or wireless paging system for global revocation from secure Web site
- Card revocation and deactivation
- Ad hoc and full-featured report generation
- Open database interfaces
- Centralized or de-centralized implementations
- Positive or negative database implementations
- Biometric capabilities
- Access control and application interfaces
- Application/container management
- Links with central processing systems

XTec, Incorporated
5775 Blue Lagoon Drive • Suite 280 • Miami, Florida 33126
Telephone (305) 265-1565 • Fax (305) 265-1569
www.xtec.com

