XTec™

Authentication and security solutions you can trust.™

AuthentX™ OCSP+

Online Certificate Status Protocol Plus

Strong authentication requires more than reading a cardholder unique ID (CHUID), verifying a digital signature and performing a cryptographic challenge-response. That's an important start, but it isn't enough to eliminate vulnerabilities. Two additional checks are essential: verifying the authenticity of the card and checking its revocation status. Agency PACS or LACS systems that overlook either are highly vulnerable to attacks from cloned, counterfeited, or revoked cards.

XTec's OCSP+ addresses this need head on. OCSP+ provides full path validation and revocation checking on digital certificates used in PIV, PIV-I, and other identity credentials. Furthermore, OCSP+ revocation checking is configurable for: use of current Certificate Revocation List (CRL), online check with the Certificate Authority (CA) and real-time feed from the issuer IDMS. The first two are standard OCSP approaches, but allow up to 18 hours latency between the time a card is revoked in the IDMS and when that information is available via OCSP.

XTec's OCSP+ capability for a real-time IDMS feed reduces that latency to milliseconds. As soon as a revocation is recorded in an AuthentX IDMS, that information is replicated in real time to OCSP+ servers. Relying parties are therefore not impacted by the latency of the revocation information from CRLs or online checks to the CA.

Deployment at the Edge

AuthentX OCSP+ supports hosted, centralized, and edge deployment. XTec offers OCSP+ as SaaS ("Software as a Service") and also provides OCSP+ hardware and software for organizations to deploy to one or more of their data centers.

It's deployment at the edge that distinguishes OCSP+, placing hardware and software geographically close to the locations where they are needed. As Agencies ramp up LACS and PACS to fully use strong authentication, OCSP+ edge-based service is key to reducing the burden on CAs and central servers, ensuring fast response times and eliminating continuous WAN connectivity as a prerequisite for availability.

AuthentX OCSP+ monitors the cardholder's location and alerts Agencies to suspicious activities, such as entering a facility immediately after logging in from a different location. The AuthentX OCSP+ may be configured to support location-specific criteria, useful particularly for locations or Agencies with a variety of visitors, PIV, or PIV-I cardholders.

Features

- Real-Time Data
- Audit & Reporting
- Physical Access Control
- Logical Access Control
- Geographic Specificity
- Increased Availability
- Supports CRL Use

Contact Us:

11180 Sunrise Valley Drive
Suite 310
Reston, Virginia 20191
(703) 547-3524
www.xtec.com

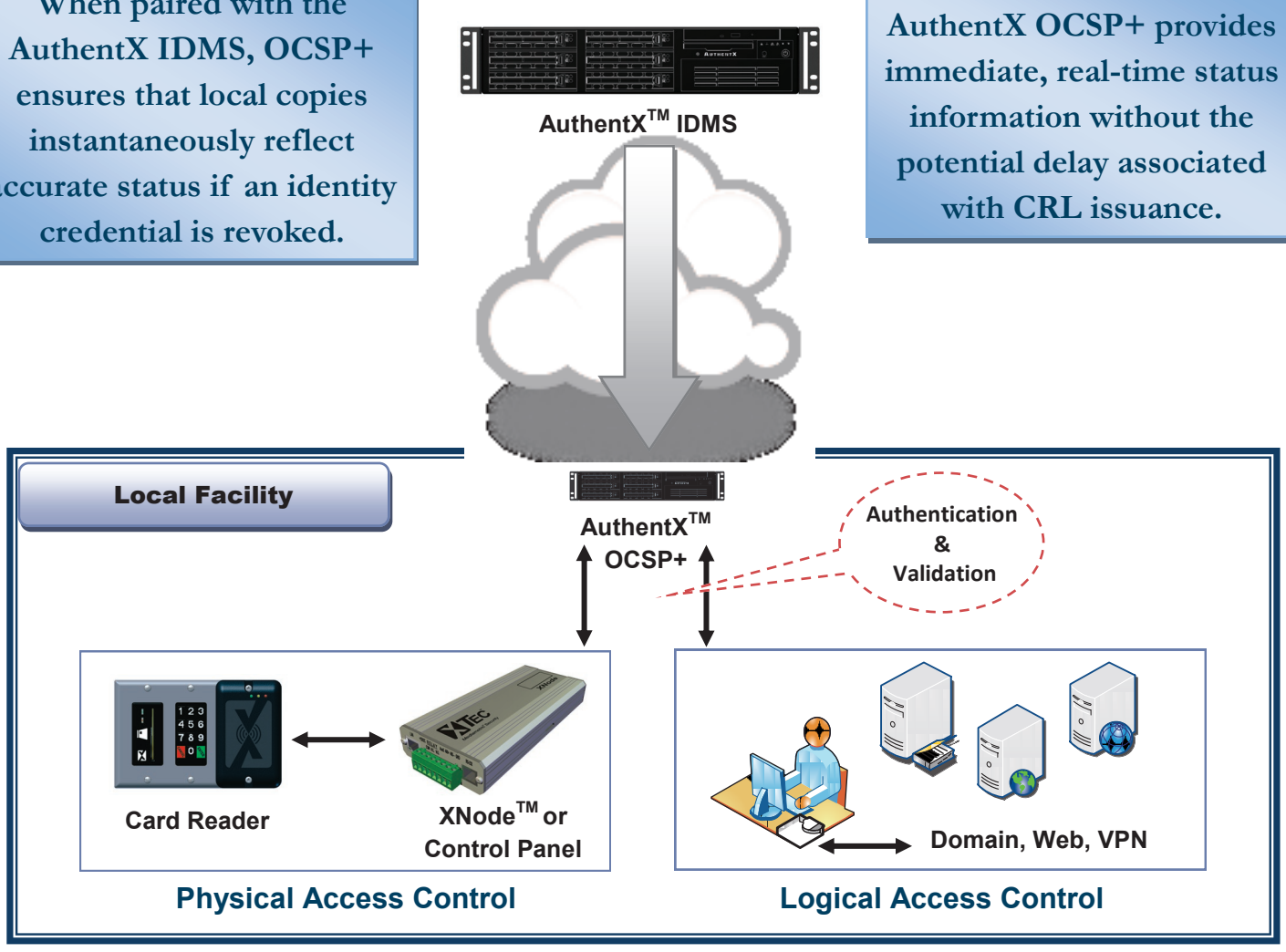
AuthentX™ OCSP+

AuthentX OCSP+ in the Enterprise

Both flexible and scalable, the AuthentX OCSP+ is rapidly deployed. It is especially useful for customers with a high concentration of employees in certain areas or dispersed among different locations. An OCSP+ module may be placed in any area where a large number of individuals are expected to utilize PKI services — for example, an area with a large number of cubicles or a main physical access point, such as the lobby. The AuthentX OCSP+ supports PIV/PIV-I certificate validation, can monitor, track, and report individual inquiries made on specific individuals.

When paired with the AuthentX IDMS, OCSP+ ensures that local copies instantaneously reflect accurate status if an identity credential is revoked.

AuthentX OCSP+ provides immediate, real-time status information without the potential delay associated with CRL issuance.



The AuthentX suite of identity products:

- IDMS/CMS
- Cloud & SaaS
- Self Service Kiosk
- Physical Access Control Solutions
- Logical Access Control Solutions
- Enrollment & Issuance Solutions
- End-to-end HSPD-12 Solution
- GSA Schedule 70 SIN 132-62
- FIPS 201 Certified Products