



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

Standard ID:	SE-ACCESS-001
Title:	Building Access Security Standard
Domain:	Security
Discipline:	Physical access
Date Updated:	6/28/2016
Revision no.:	5
Original date:	11/17/2009

I. Authority, Applicability and Purpose

- A. **Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information to implement statewide and interagency technology solutions, policy, standards and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store and disseminate information or data electronically. The term "technology" includes systems and equipment associated with e-government and Internet initiatives.
- B. **Applicability:** Applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, and continued use of these resources.
- C. **Purpose** – The purpose of this standard is to establish consistency in both the quality and the security of building access controls for State of Delaware facilities except school districts and correctional/security facilities. It will meet the needs of the Division of Capitol Police regarding building access, occupant identification and emergency access.

II. Scope

- A. **Audience:** – This document is intended for IT personnel in State facilities, except school districts, that are responsible implementing security mechanisms for buildings.
- B. **Applicability** – This standard will cover all State facilities except school districts and correctional/security facilities.
- C. **Areas Covered** – This standard will address the type of cards to be used for secure access to State facilities except school districts and correctional/security facilities. Also, it will address the type of building security management system to be deployed in State facilities except school districts and correctional/security facilities.

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

- D. **Environments** – With the exception of school districts and correctional/security facilities, building access controls will be deployed in all State facilities that require restricted or managed access.

III. Process

- A. **Adoption** – These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.
- B. **Revision** – Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review each standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).
- C. **Contractors** – Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@state.de.us.
- D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement this standard during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.
- E. **Enforcement:** DTI will enforce this standard during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This standard may also be enforced by others during the course of their normal business activities, including audits and design reviews.
- F. **Contact us** – Any questions or comments should be directed to dti_tasc@state.de.us.

IV. Definitions/Declarations

A. Definitions

1. **Contactless card:** A smart card that uses radio frequencies to exchange information. Unlike a contact card, it needs no physical contact to be read by readers or terminals. Containing an embedded integrated circuit known as a "contactless chip," the card needs only to be waved near a reader to record transactions or to identify the user. Contactless-card systems are either passive, with the readers generating the frequency, or active, in which the card activates the reader.¹
2. **Corporate 1000 Program:** The Corporate 1000 Program card numbering scheme allows for a card format that is developed specifically for each individual end-user customer. Card numbers are tracked in the manufacturing process to ensure that card numbers are not duplicated.

¹ Gartner, Inc -- http://www.gartner.com/6_help/glossary/GlossaryMain.jsp



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

B. Declarations

1. Must support a 13.56Mhz contactless card
2. Must be a part of the **Corporate 1000 Program**.

V. Definition of Ratings

COMPONENT RATING	USAGE NOTES
<p>STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle.</p>	<p>These components can be used without explicit DTI approval for both <u>new projects</u> and <u>enhancement</u> of existing systems.</p>
<p>DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.</p>	<p>Via the State’s waiver process, these components must be explicitly approved by DTI for <u>all projects</u>. They must not be used for <u>minor enhancement</u> and <u>system maintenance</u> without explicit DTI approval via the State’s waiver process.</p>
<p>DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.</p>	<p>No waiver requests for new solutions with this component rating will be considered.</p>

- A. Missing Components** – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.



DELAWARE STATE-WIDE INFORMATION TECHNOLOGY AND ARCHITECTURE STANDARDS

VI. Component Assessments

Component	Rating	Comments
<u>Building Access Security Card</u>		
HID Proximity 125kHz	Declining	Acceptable only for organizations with existing readers that accept ONLY HID Proximity 125kHz cards. 125KHz technology is being phased out. Must be a part of the Corporate 1000 program.
iCLASS® 13.56MHz	Standard	iCLASS technology only or multi-technology form factor with HID 125kHz proximity. Multi-technology cards should be used for organizations that still have 125kHz card readers. This enables future migrations to the more secure iCLASS readers without needing to re-purchase cards/credentials. Must be a part of the Corporate 1000 program.
Any card NOT purchased through the State of Delaware Corporate 1000 program	Disallowed	Cards purchased through the State of Delaware Corporate 1000 program ensure no duplication of credentials.
<u>Combination Physical and Logical Access Cards</u>		
Crescendo	Standard	To be used when a single card for logical and physical access is required. Must be a part of the Corporate 1000 program.
<u>Card Readers</u>		
iCLASS SE or MultiCLASS SE	Standard	Must be compatible with the existing cards. SE readers can be field upgraded to support future SEOS technology while still backwards compatible.
Proximity 125KHz	Declining	Phasing out 125KHz cards
<u>Building Security Management System</u>		
Pro-Watch®	Standard	Authorized Pro-Watch® vendors in Delaware

These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.