CPNI
Centre for the Protection of National Infrastructure

Automatic Access Control System Tokens and Readers

A Procurement Guide

September 2014

About this document

This document has been produced by CPNI to give guidance suggesting a list of key security principles to be considered when procuring Radio-Frequency Identification (RFID) smartcards and readers for Automatic Access Control Systems (AACS). It is written as advice for areas of HMG, the Critical National Infrastructure (CNI), their agencies and suppliers.

About AACS

An Automatic Access Control System is an electronic system controlling entry into and/or exit from a specified area.

Smartcards securely store a secret unique user ID which is transferred to a reader over a secured RFID communications link. The reader then delivers the user ID which when combined with a separate typed-in user PIN provides authentication to the AACS combiner.

Key security principles

The following security principles should be considered when procuring AACS comprising of smartcards, or tokens, and readers.

Principle 1	**Protect user ID in transit**
Why this matters	Interception of sensitive data in transit could allow unauthorised site access.
Recommendations	• Transfer of the user ID from the smartcard to the reader should be protected using encryption. • The above authentication and encryption should be based on known good cryptographic standards (see NIST SP 800-57 part 1 and NIST SP 800-131A, available at csrc.nist.gov). • Where such standards are not used, the supplier should provide evidence to show that the cryptographic mechanisms and algorithms used are suitable. Note: This task is likely to be non-trivial. • Note: Communications between the reader and the AACS controller should be protected in line with general CPNI AACS system guidance.

Principle 2	Protect sensitive data at rest
Why this matters	Unauthorised access to sensitive data on a compromised device could allow unauthorised site access.
Recommendations	• The smartcard should only transmit its user ID (via an encrypted link) after the reader has been successfully authenticated by the smartcard. • The smartcard should otherwise generally prevent sensitive data being trivially accessed. (Note: external certification, such as Common Criteria, can help to provide evidence of such protection.) • The reader should not retain any sensitive data (user credentials or cryptographic material), other than a reader key if required (stored in a part of the reader, located inside the site perimeter). • The user PIN should not be stored on the smartcard – to protect against loss of smartcard compromising both user ID and PIN.

Principle 3	Secure externally-accessible reader hardware
Why this matters	Undetected reader tampering could allow authorised access to user IDs and PINs. Unsecured reader interfaces/ports could allow unauthorised access to sensitive data.
Recommendations	• The externally-accessible part of the reader should be manufactured so that any unauthorised tampering is evident during a security audit. • The externally-accessible part of the reader should not expose any interface ports that could allow unauthorised access to (or modification of) sensitive data, either within the device or wider site systems. • Note: Sensitive data here also includes reader firmware.

Principle 4	Minimise impact of compromise
Why this matters	Compromise of a smartcard holding cryptographic material shared with other devices could result in wider AACS compromise.
Recommendations	• The sharing of sensitive key material (e.g. private keys, symmetric keys, etc.) between multiple smartcards should be avoided. • Similarly, a smartcard should not store sensitive reader key material. • As stated elsewhere, a reader should not retain any cryptographic material other than its own key.

Principle 5	Use trusted smartcard provisioning and support
Why this matters	Lack of trusted smartcard/PIN management (provisioning, revocation, re-issuing, etc) risks unauthorised persons gaining access to sensitive user access control details.
Recommendations	• If sensitive smartcard data (key material and User Identifiers) and user PINs are not generated and managed locally, a trusted source should be used to do this. • Similarly, a trusted source should also be used to manage any external escrow arrangements. • If smartcard provisioning is being undertaken by a third party, consider service level agreements and emergency provisioning plans for use in business continuity emergencies. • Note: Careful consideration should also be given to the general acquisition of readers and smartcards through a trusted supply chain.