National Protective Security Authority

User Guide on Token and Reader Procurement

(EIS0004)

Disclaimer

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Contents

1 Introduction

1.1 Overview

This document has been produced by NPSA to give guidance on key security principles to be considered when procuring Radio-Frequency Identification (RFID) tokens and readers for Automatic Access Control Systems (AACS).

Something we have

1.2 Scope of Document

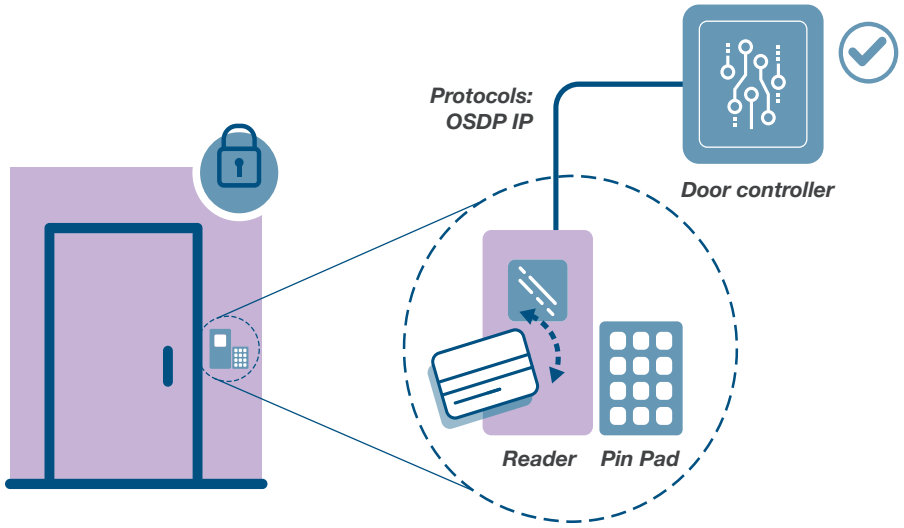
This document provides high-level guidance on token and reader procurement. It is divided into the following sections:

1. Introduction
2. About AACS
3. Key Security Principles

2 About AACS

An Automatic Access Control System (AACS) is an electronic system controlling entry into and exit from a specified area.

Tokens 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.



1. A security credential is presented to a reader.

2. The reader reads the credential and sends a signal to the door controller, which authenticates the credential. If a pin is included in the design, the user enters the pin and sends it separately to the door controller.

3. If authenticated, the door lock is released. If not, the door remains locked.

3 Key Security Principles

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

3.1 Principle 1: Protect User ID in Transit

Interception of sensitive data in transit could allow unauthorised site access.

Transfer of the user ID from the token 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.

Communications between the reader and the AACS controller should be protected in line with general NPSA AACS system guidance.

3.2 Principle 2: Protect Sensitive Data at Rest

Unauthorised access to sensitive data on a compromised device could allow unauthorised access.

The token should only transmit its user ID (via an encrypted link) after the reader has been successfully authenticated by the token.

The token 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 secure part of the reader, located inside the site perimeter).

The user PIN should not be stored on the token – to protect against loss of token compromising both user ID and PIN.

3.3 Principle 3: Externally Accessible Reader Hardware

Undetected reader tampering could allow unauthorised access to user IDs and PINs. Unsecured reader interfaces could allow access to sensitive date.

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.

Sensitive data here also includes reader firmware.

3.4 Principle 4: Minimise Impact to Compromise

Compromise of tokens holding cryptographic material shared with other devices could result in wider AACS compromise.

The sharing of sensitive key material (e.g. private keys, symmetric keys, etc.) between multiple tokens should be avoided.

Similarly, a token should not store sensitive reader key material.

As stated elsewhere, a reader should not retain any cryptographic material other than its own key.

3.5 Principle 5: Use Trusted Token Personalisation and Support

Lack of trusted token/PIN management (personalisation, revocation, re-issuing, etc.) risks unauthorised persons gaining access to sensitive user access control details.

If sensitive token 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 token personalisation is being undertaken by a third party, consider service level agreements and emergency provisioning plans for use in business continuity emergencies.

Careful consideration should also be given to the general acquisition of readers and tokens through a trusted supply chain. See NPSA website for further guidance on supply chain security for suppliers".

4 Summary

This guidance document has provided an overview of Token and Reader Procurement. The content can be summarised as follows:

Key Points

1. Interception of sensitive data in transit could allow unauthorised site access.
2. Access to sensitive data on a compromised device could allow unauthorised access.
3. Undetected reader tampering could allow unauthorised access to user IDs and PINs.
4. Unsecured reader interfaces could allow access to sensitive data.
5. Compromise of tokens holding cryptographic material shared with other devices could result in wider AACS compromise.
6. Lack of trusted token/PIN management (provisioning, revocation, re-issuing, etc.) risks unauthorised persons gaining access to sensitive user access control details.

Further Information

Further advice and supporting guidance documents are available through the relevant NPSA adviser, or from the NPSA website **www.npsa.gov.uk.** Further reading is available on the following related subjects:

- Automatic Access Control Systems
- Token and Reader Technology
- Operational Requirements for Security Measures
- The Catalogue of Security Equipment
- Supply Chain Security for Suppliers
- Equality Act - available from gov.uk
- Data Protection Act - available from gov.uk