CPNI
Centre for the Protection of National Infrastructure

Access Control Token – Visual Design Guide

PUBLISH DATE: July 2021

CLASSIFICATION: Official

Automatic Access Control Token – Visual Design Guide

Version 1.0

Introduction

Automatic Access Control Systems (AACS) can provide a secure and auditable method of controlling access into a secure premise. While the AACS and its underlying infrastructure should be secured to a suitable level, the token (often called a user's "Pass") should also be robust, both technologically and visually. CPNI has assurance schemes for AACS's, Cyber Assurance (CAPSS), Readers, Keypads and Tokens. While these standards cover the technical aspects of assurance, they do not cover the visual features of the token.

This guidance document provides guidance for the design and layout of an AACS token, when used on a secure site.

Token Features

An AACS's biggest vulnerability is its expectation handling process. What are the policies and procedures that are undertaken when the AACS does not function as intended? Using a seemingly legitimate, although non-functioning, AACS token to socially engineer access to a secure site is a powerful attack methodology and is only successfully mitigated by good token design and secure policies and procedures.

All AACS tokens should be able to provide a number of security features which when correctly checked will be able to highlight a forged AACS token.
Tokens should have at least:

- **A high-quality photo of the passholder**
- **Non-standard colours i.e. not "pure" red, green or blue used for printing (see section below for further**
- **An intricate, high quality, logo on the front of the token, ideally not tied to the organisation that issued the token**
- **A returns address on the read of the token, ideally not revealing the location the token grants access to**
- **An expiry date**
- **Large wording to denote the function of the passholder i.e. CONTRACTOR**
- **A holographic laminate applied to the front of the card, over all printing**

The above features can be further bolstered with the following additional security features:

- **Raised writing on the rear of the card**
- **A logo overlapping the pass holder's picture**
- **Colours, symbols or letters indicating the pass holders home department or building**

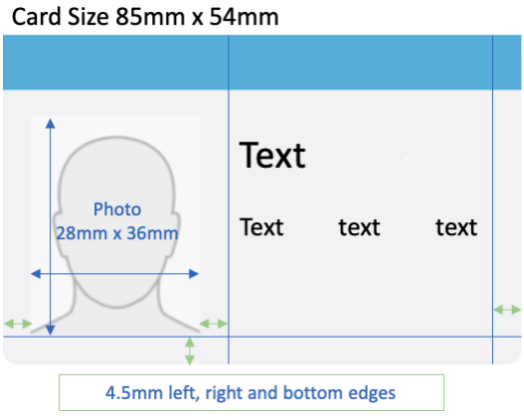
Token Design

The following are representative designs for two levels of AACS tokens. The first design is the recommended minimum standard to achieve a secure token, the second design is the recommended standard for a token used on a high security site. Each token design implements a number of security features which, when coupled with a secure authentication process, will allow confidence in the authenticity of the token.

Minimum Design Specification

To ensure that the pass design is visually and physically difficult to copy, it is recommended that the following features are implemented as a minimum in any access control token.

A high-quality photo of the passholder



The photo should aid identification and enable a security officer to confirm the holder of the token is the legitimate user. The photo should be of **good quality** and should only contain a **close-up of the full head** of the user.

Photos should be:

- **36mm high by 28mm wide**
- in colour
- taken against a plain cream or light grey background
- clear and in focus
- facing forward and looking straight at the camera
- with a neutral expression and your mouth closed
- without anything covering the face
- in clear contrast to the background
- without a head covering (unless it's worn for religious or medical reasons)
- with eyes open, visible and free from reflection or glare from glasses
- with your eyes not covered by sunglasses, tinted glasses, glasses frames or hair
- without any shadows in the picture

Non-standard colours i.e. not “pure” red, green or blue used for printing

Standard colours are easier to match and clone than non-standard colours, therefore ‘**bespoke’ colours should be utilised** where possible. When a pass is verified the colour of features on the pass play an important role in identifying a illegitimate token.

Examples of difficult to match colours may include:

R:77 G:97 B:116

R:68 G:128 B:198

R:94 G:209 B:120

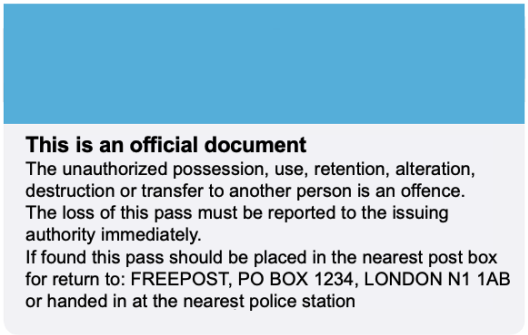
An intricate, high quality, logo on the front of the token, ideally not tied to the organisation that issued the token

Intricate designs are difficult to scan or copy and when compared against a known ‘good’ example can highlight printing defects. The design used for the logo should **not be freely available on the internet** to download.

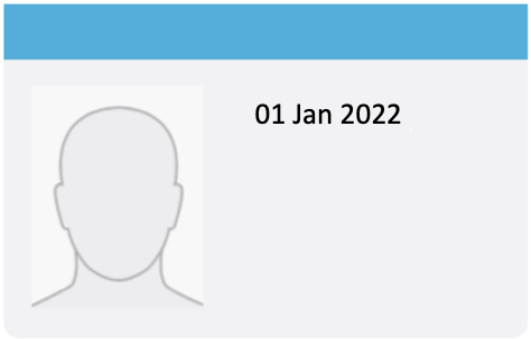
An example of a high quality (although readily available) logo would be:

A returns address on the read of the token, ideally not revealing the location the token grants access to

Lost tokens discovered by those outside the organisation should be returned to the issuing organisation. To enable this a returns address should be provided on the rear of the token. If this address is a valid site which the token may grant access to, an opportunistic attacker could leverage this to form a chance attack. Therefore, the return address should be a separate site or ideally an anonymous Post Office **(PO) box**. The return address needs to be supported by policies such as having a PO box or an agreement with the Police on how to deal with lost tokens.



An expiry dates



The expiry date of the token should be clearly printed on the front. This will enable both security officers and staff members to undertaken rudimentary checks for expired passes

Text should be **size 14** print to enable reading from a distance.

Large wording to denote the function of the passholder i.e. CONTRACTOR

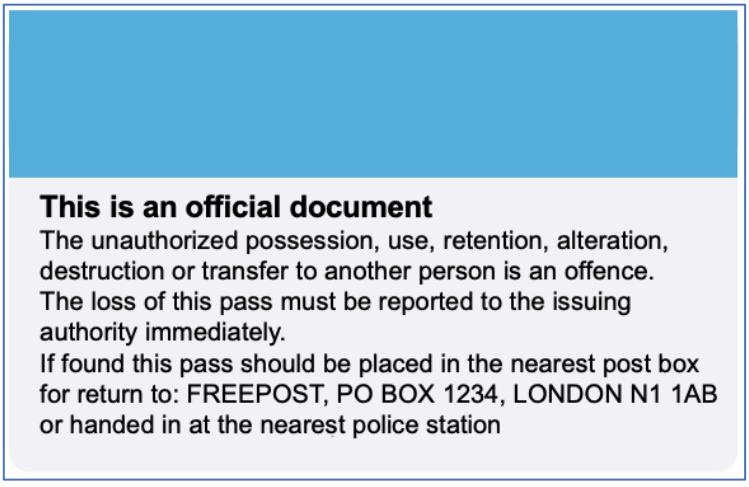
Where an organisation issues different types of tokens, potentially with restricted access, this should be clearly denoted on the token. Examples of this might include VISITORS, EVENTS, CONTRACTORS or TEMPORARY passes.

Text should be **size 14** print to enable reading from a distance.

A holographic laminate applied to the front of the card, over all printing

Holographic laminate overlays act as a form of tamper indication for tokens. Applying an overlay to the token minimises wear on the token, protects the print and quality of the token and **assists in identifying tamper** to the token

A complete 'Minimum Specification' card



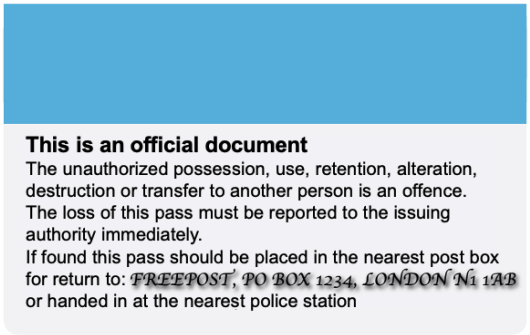
Higher Security Design Specification:

On top of the 'minimum design specification' detailed above, the following items can be added to increase the visual security of the token.

Raised writing on the rear of the card

Raised writing is likely to add a significant burden to those looking to copy a token. The vast majority of those looking to copy an access control token will not have the ability to produce a card with raised writing.

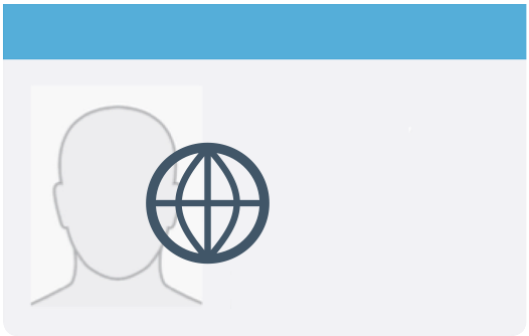
Raised writing does not need to be accessible every day and can be used as a secondary check when confirming the authenticity of a card. The raised writing can be on the rear of the card to protect it from wear.



It is recommended that a common feature amongst all cards produced on site is chosen for the raised writing, this means the raised writing can be done in bulk rather than custom for each card.

The writing should be at least **size 10** print.

A logo overlapping the pass holder's picture

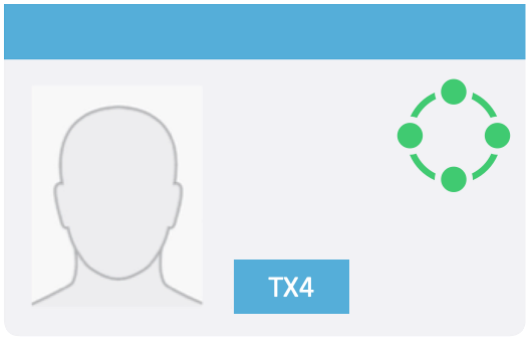


Logos overlapping photos originate from when separate photos were attached to ID cards, however there is still benefit in applying one to a token which has the photo printed on. Removing the photo and printing a new picture could be undertaken by those looking to copy a token. Adding a logo in a non-standard colour, would require colour matching of the existing logo and risks wider damage to the token, thus indicating a tampered with card.

The logo should cover approximately **half the height, and one quarter width, of the photo**.

Colours, symbols or letters indicating the pass holders home department or building

Where necessary it may be used to provide a visual identification of areas where the token holder is legitimately allowed to access or their 'home department'. This assists with good personnel security processes and a strong security culture of challenging those out of their permitted areas.



Departments should be represented via codes or symbols, rather than overt names

Text or symbols should be **size 14** print (or equivalent) to enable reading from a distance.

A complete 'Higher Security' card