



Mifare® Classic Customer Media Phase Out – Questions & Answers

Question	Answer
<p>What impact does this phase out have upon current cards operating in the ITSO environment?</p>	<p>None. This is a pro-active phase out which focuses on future card issues after 31st December 2009. All Mifare® Classic media operating across the ITSO environment remains fully supported until 31st December 2016, guaranteeing support for all current media for the duration of their operational period.</p> <p>This is a justified decision which takes on-board the theoretical risk posed by Mifare® Classic security issues, despite posing no immediate threat to the ITSO environment.</p>
<p>Are current Mifare® Classic cards operating in the ITSO environment safe?</p>	<p>Yes. Every card operating in the ITSO environment is required to operate with additional ITSO security. Potentially, this means that if any intentional attempts are made to defraud a card this can be tracked and identified. Again in terms of the English National Concessionary Travel Scheme (ENCTS), ITSO would like to re-emphasise the need for stop listing data to be continually provided by TCAs in order to root out fraudulent cards from the field.</p> <p>Furthermore, additional identification features such as photo ID and holograms on ENCTS cards ensure that highly competent security measures are in place.</p>
<p>What if Mifare® cards are issued after 31st December 2009?</p>	<p>These will not be supported in the ITSO environment, this would mean that smart transactions cannot be registered.</p>
<p>How many Mifare® Classic media are operating in the ITSO environment currently?</p>	<p>There are some 7.2 million Mifare® Classic media operating in ENCTS, with a further 1.4 million operating in the Scottish Entitlement Scheme and some 0.5 million in the Welsh concessionary scheme.</p>
<p>Is personal data on Mifare® Classic card media at risk from threats such as card cloning?</p>	<p>No personal data is stored on individual ENCTS cards and additional security measures put in place by ITSO (particularly with the back office system) means that personal data is not at risk. Whilst the holding of personal data can vary per concessionary scheme, ENCTS has recommended that no individual's details are retained within its scheme.</p>
<p>What threat has been identified by ITSO specifically?</p>	<p>The Mifare® Classic range of smartcards (Mifare 1k and Mifare 4k) are unusual in the ITSO environment in that they use proprietary cryptography that ITSO are unable to verify. Recent published evidence from University College London indicates that it is now possible to crack the Mifare® Classic cryptography within two minutes and clone the card onto an emulator built using standard components available over the internet.</p> <p>However ITSO only use the Mifare® cryptography as a means to communicate with the card and the Products are independently protected</p>



	by the ITSO seal which uses different and more secure cryptography. For some ITSO Licensed Members' schemes further physical security exists in the photo on the card plus the overlay of a hologram.
Will I need to order new stocks of alternate card types?	If you intend for those cards to be printed and encoded before 31 st December 2009, no. Anything created for use in the ITSO environment after this date will not be supported, therefore new stocks will be required for issues on or after 1 st January 2010.
Is there a preferred card alternative option?	No, the decision is left to own discretion.
How does the recent memo from ITSO regarding CMD2 impact upon this?	ITSO have recently stated their intentions to phase out all CMD2 media that does not meet a minimum transaction time of 6000ms, this is based on the same timescale as the Mifare® Classic phase out. This does not mean that all CMD2 media is intended to be phased out, rather the intention is to induce faster transaction times into the ITSO environment.
Will there be any future dialogue from ITSO on this matter?	ITSO will stage a workshop in the last week of January to discuss the matter further, this will be held in association with ITSO Services. Further information on this workshop will be released shortly.
Have the Department for Transport been informed of this statement?	Yes, ITSO, and ITSO Services in their role as licenced operator within ENCTS, are working very closely with the DfT on this issue.
What impact does this have upon POSTs (Electronic Ticketing Machines on board buses?)	All ITSO POSTs will need to be compliant with all forms ITSO certified card media. POST providers are required to provide this and will be able to provide further information; as well as any technical updates that may be required as a matter of course.
What impact does this decision have on other card applications?	It should be noted that the LASSeO local application specification is anticipated to be ready by the end of 2008. LASSeO are aware of this ITSO statement and are planning action in conjunction with this. Existing Electronic Ticketing Machines may need to be updated, for further information please contact your card supplier.
Does this statement impact upon a card holder?	No, the passholder will see no difference in the functionality of their pass, be it as a flash pass or within a smart environment.