Sharing MIFARE® DESFire cards between sites

Overview Document

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

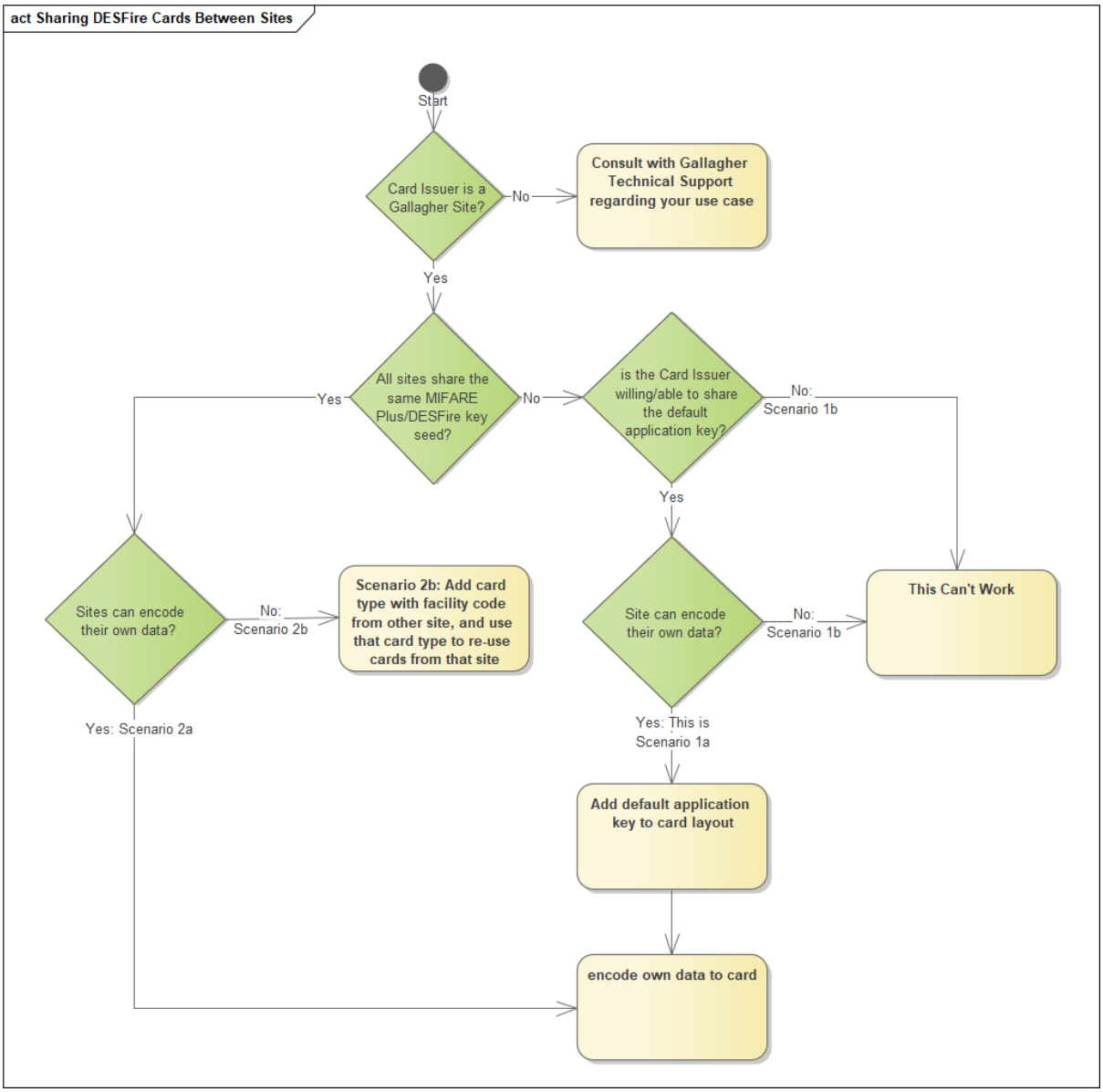
Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2020. All rights reserved.

1 Terms and Definitions

Term	Definition
Original Card Issuer	This is the organisation that initially encodes the card.
Secondary Site	This is a site that wants to enable a card (originally issued by a different organisation) to work with their system.
Card Application	This is an independent entity on a DESFire card that has separate access control and is protected by its own keys.
Default Application Key (DAK/PICC App Default Key)	This is the value that the keys for a new card application are set to by default, before the application creator changes them to something more secure. If an original card issuer is happy to let other sites encode independent card applications to cards that they have issued, then this is safe to share with the other organisations. This is found in the Card Security tab of the server properties in the Configuration Client.
MIFARE Plus/DESFire key seed	A value used as the seed to derive keys used to protect each card. This is found in the Card Security tab of the server properties in the Configuration Client.

2 Determining how to share cards



3 Sharing Scenarios

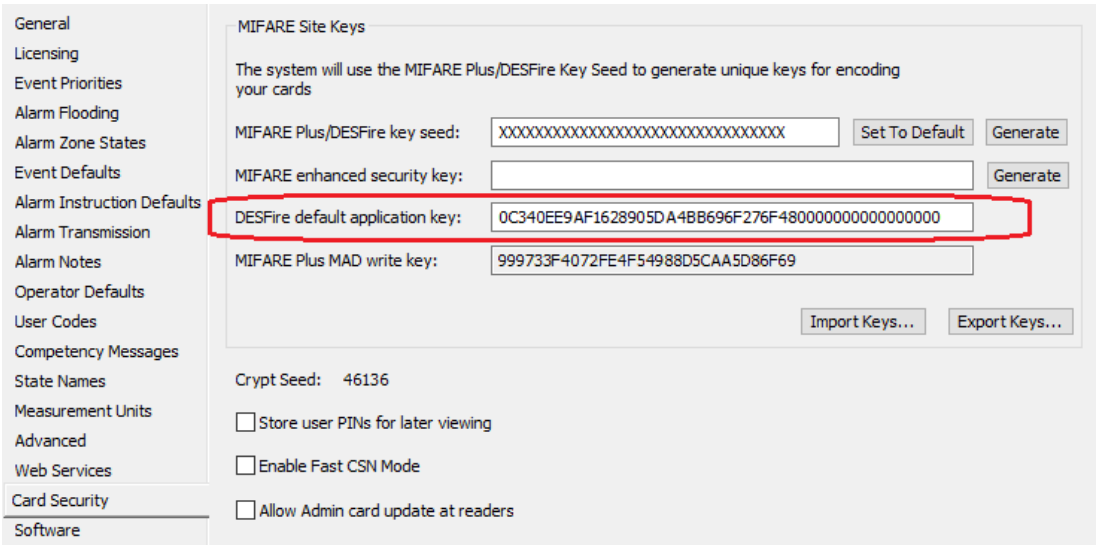
This section describes various scenarios where a site is trying to use DESFire cards issued by a third party – this third party may or may not be another Gallagher site.

Scenario 1: Two Gallagher Sites that aren't able to share a MIFARE Plus/DESFire Key Seed

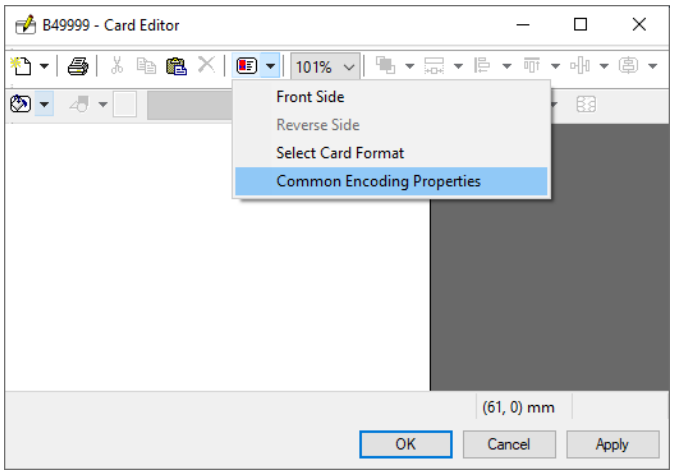
<u>Scenario 1a</u>: The Original Card Issuer is willing and able to share the Default Application Key and the Secondary Site can encode cards

The original card issuer copies the Default Application Key from the Card Security tab of the Configuration Client Server Properties and shares it with the Secondary Site:

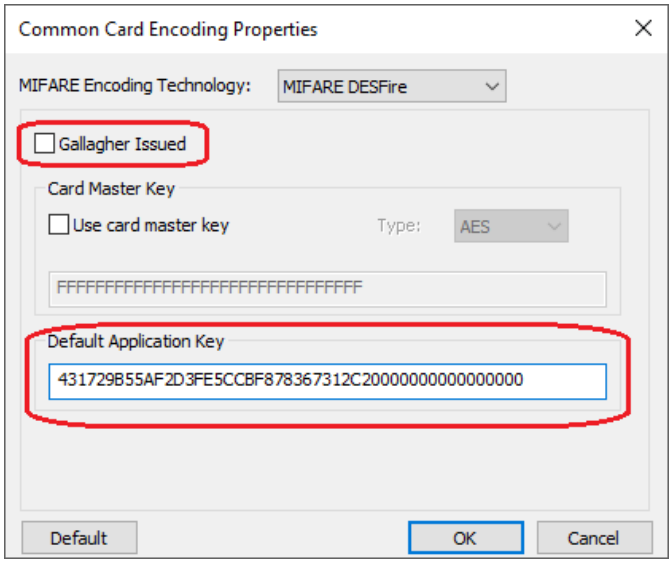
Copyright © Gallagher Group Limited



The Secondary Site then creates a new card type, and in the Common Encoding Properties of the card layout:



Then untick "Gallagher Issued" and enter in the Default Application Key:



The Secondary Site then encodes cards using that card type.

Copyright © Gallagher Group Limited

Scenario 1b: The Original Card Issuer is willing/unable to share the Default Application Key and/or the Secondary Site can't encode cards

This scenario is not supported.

Scenario 2: Both parties are Gallagher sites with the same MIFARE Plus/DESFire Key Seed

This shared key could initially either be the same or it could be a key seed that the original card issuer was willing to share with the secondary site.

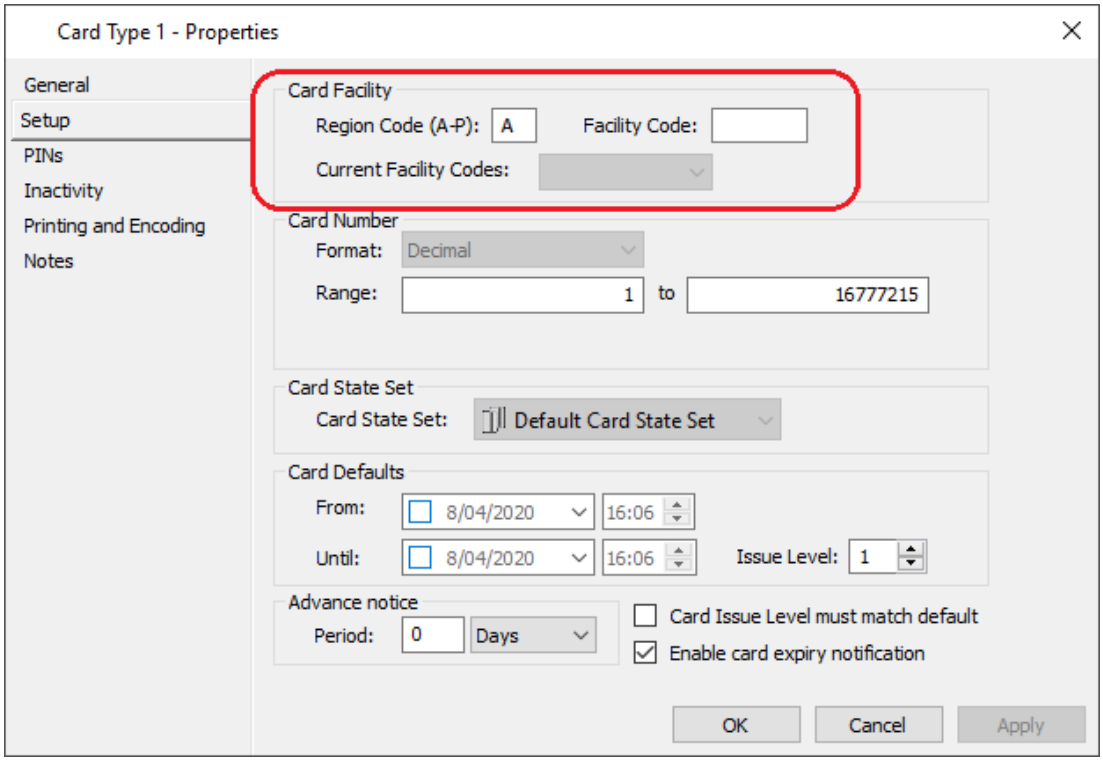
Note: Sharing the MIFARE Plus/DESFire Key seed between different sites should not be done unless there is a high degree of trust between the sites, e.g. they are part of the same organisation.

Scenario 2a: The Secondary Site can encode cards

In this case the Secondary Site can just encode the cards as they normally would, and things will just work.

Scenario 2b: The Secondary Site can't encode cards

In this case the original card issuer provides their facility code to the Secondary Site, who creates a new Card Type using the provided facility code:



The Secondary Site then uses that card type when adding cards to a cardholder who had their card issued by the original card issuer – though because they're re-using the existing data encoded to by the original card issuer the card number that they add must match what is already encoded on the card.

Copyright © Gallagher Group Limited