Table des matières

Bypass BIOS PASSWORD 2
Bios 2
eMMC 2
BOOT 4
Windows 6

Bypass BIOS PASSWORD

Comment contourner le mot de passe d'un bios codé pour booter sur un media externe.
Dans beaucoup de cas le boot usb n'étant pas possible, il vous faudra contourner cette restriction.

Voici comment faire.

Dans ce tutoriel, le poste cible ne possède pas de chiffrement BitLocker, le disk est de type eMMC (donc HotPlug!) et le BIOS est codé sans boot possible sur support via usb.

Bios

Il vous faudra démonter le châssis du pc portable pour accéder à la carte mère et identifier la puce eMMC.

eMMC

Ci-dessous le datagramme de puce type eMMC:

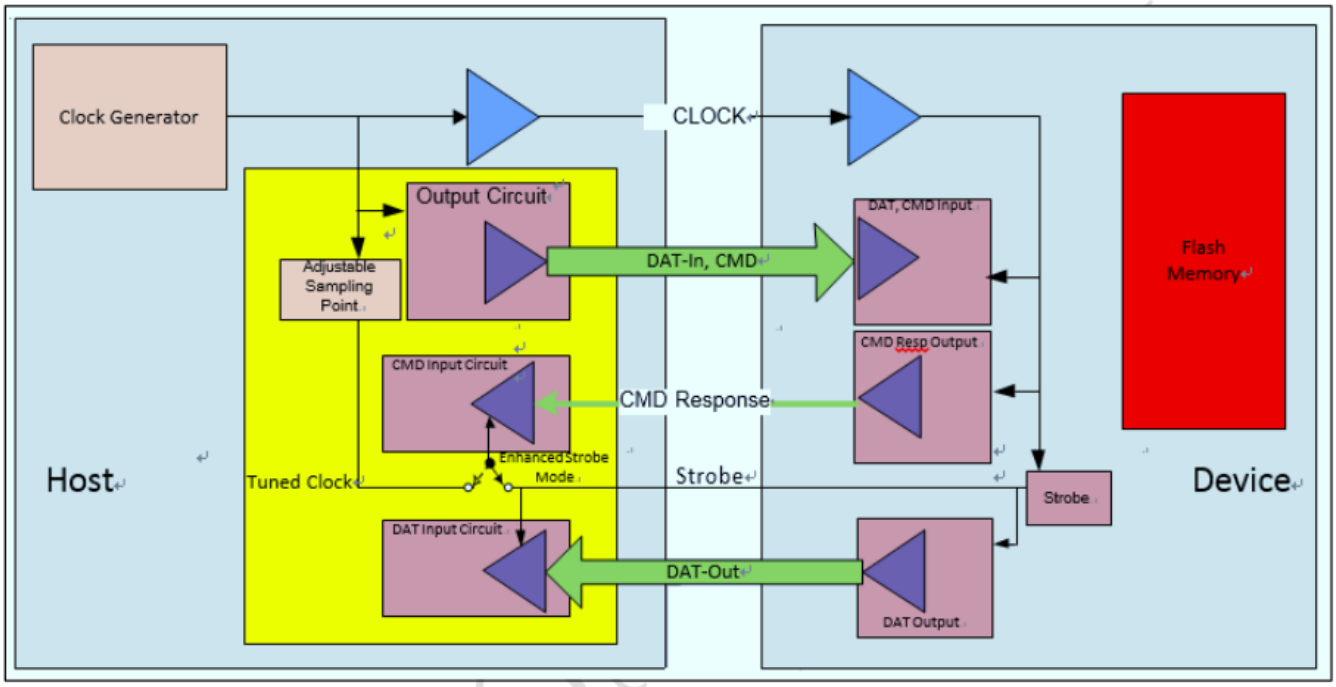


Figure 3- HS400 Host and Device block diagram

On observe ici les 8 Bus de data

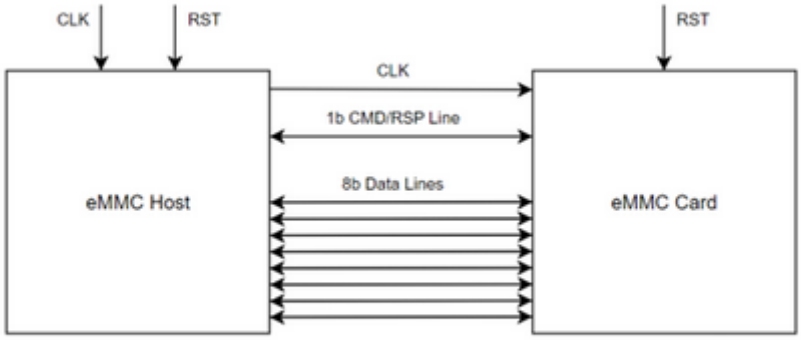


Figure 2: eMMC Architecture

Table 4– Communication Interface

Name	Type[1]	Description
CLK	I	Clock
DAT0	I/O/PP	Data
DAT1	I/O/PP	Data
DAT2	I/O/PP	Data
DAT3	I/O/PP	Data
DAT4	I/O/PP	Data
DAT5	I/O/PP	Data
DAT6	I/O/PP	Data
DAT7	I/O/PP	Data
CMD	I/O/PP/OD	Command/Response
RST_n	I	Hardware reset
VCC	S	Supply voltage for Core
VCCQ	S	Supply voltage for I/O
VSS	S	Supply voltage ground for Core

Vu réel issue d'une Carte Mère

On voit donc ici les fameux bus de données!! C'est là que la magie opère !!

L'objectif ici sera de faire croire au system que le disk n'y est plus !!
Définition:
`L'eMMC (Embedded Multi-Media Card, carte multimédia embedded) est une solution de stockage SMT soudée pour les applications à espace limité.`
Ce type de module est Hot Plug !!

BOOT

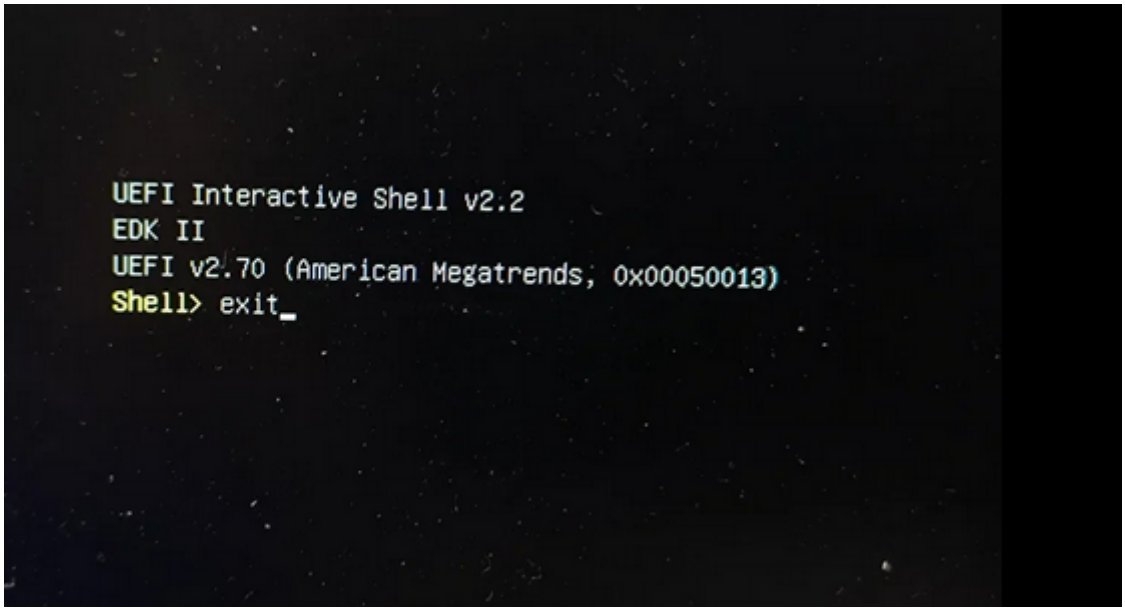
Afin de contourner la sécurité du BIOS et nous permettre de booter sur un media type USB, nous allons court-circuiter le module eMMC en shuntant 2 pin du BUS data !!

Préparer votre clé Usb boot avant, exemple Dart10 ou Win11 installation.
Pour aller plus loin et reset complètement le bios (réécrire), nous pouvons telecharger le binaire de l'utilitaire de mise à jour du BIOS et l'injecter dans une image Win PE pour être exploitable !
De ce fait une fois le boot effectué sur le media, nous pourrons donc flasher le bios et ainsi effacer le mot de passe !!

Noter que le court-circuit se fait sur 2 pin et bien coté puce, pour éviter de causer des dégat coté MB.

1. Brancher votre clé usb sur le poste
2. Faire contact entre 2 pin (rester le temps du boot)
3. Allumer le pc
4. Le boot devrais amorcer le support Usb (arreter le court-circuit)

Dans certain cas, vous pouvez vous retrouver sur la mire UEFI, il vous suffira de saisir `Exit` pour sortir de l'assistant UEFI.

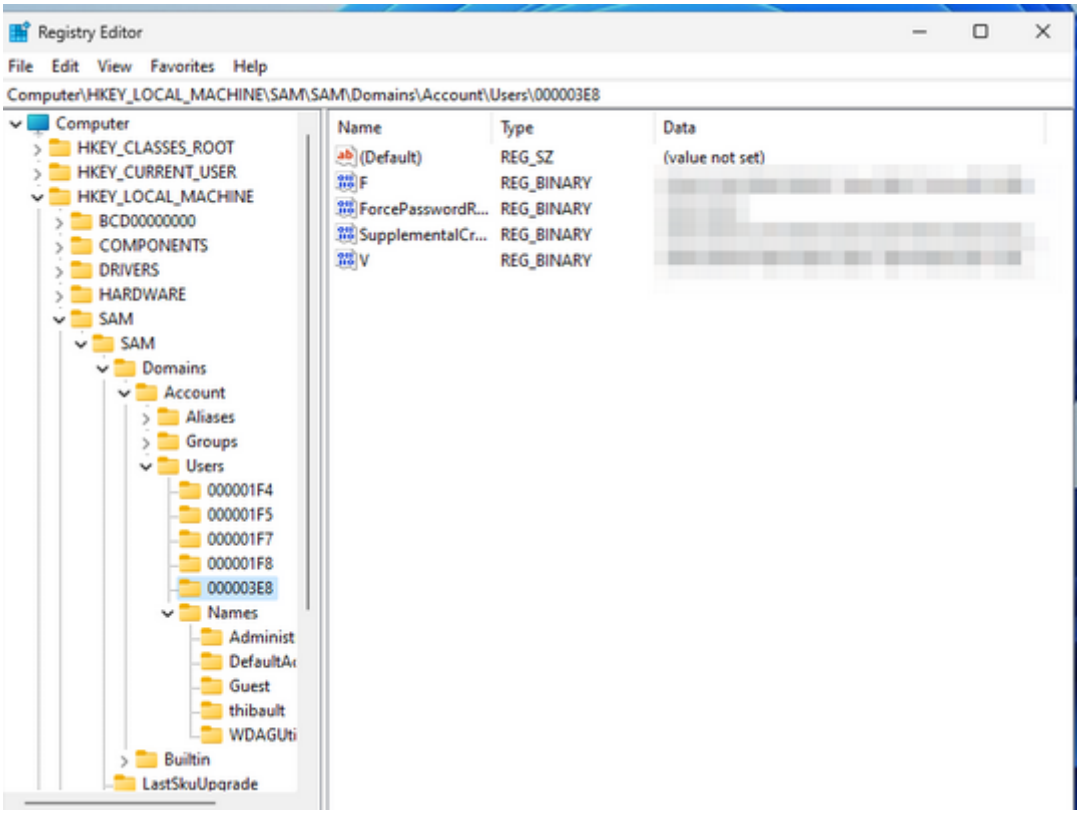


Windows

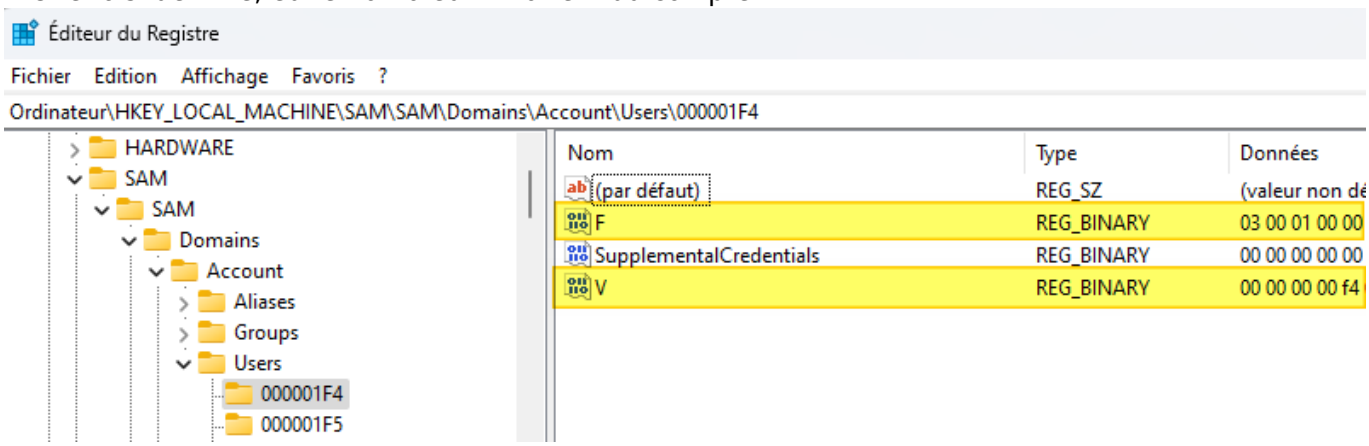
Ré-Activé le compte administrateur

Souvent désactivé pour des questions de sécurité.

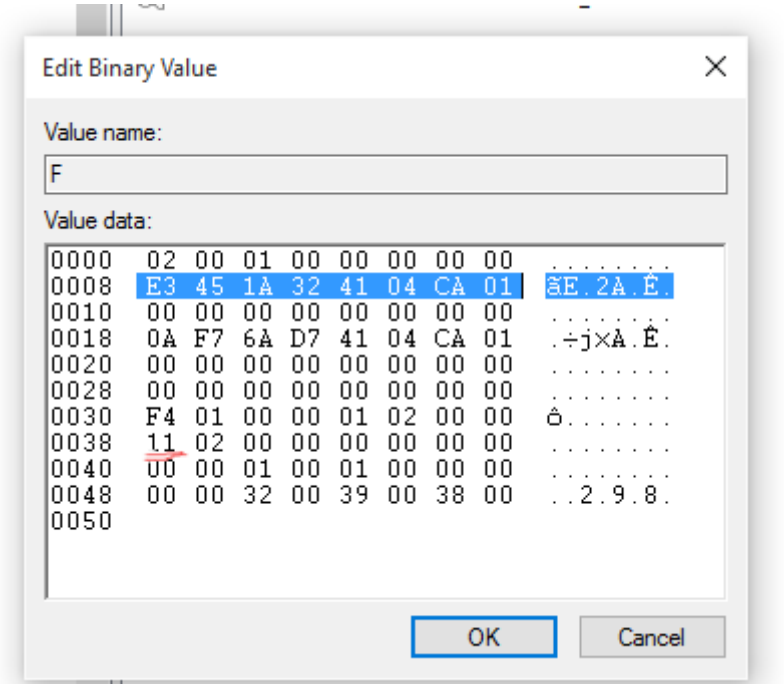
Dans le cas d'un boot sur un DART10 (suite Sysinternals), executer l'editeur de registre Windows.
Aller dans la ruche HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Accounts\Users.



Identifier le compte Administrateur en vous aidant du sous conteneur NAMES pour récupérer l'ID du compte.
**Une fois identifié, editer la Valeur Binaire F du compte.



Modifier le 8em Octect HexaDecimal de `11` qui correspond à `Désactivé` à `10` pour `Activé`



Pour la suite, un petit coup de LockSmith ou Serrurier pour reset le password du compte Administrateur !
