Traitement de données

Utilisation des cartes à puce : programmation des échanges

Objectifs.

On se propose dans ce TP de comprendre la mise en œuvre et la programmation des échanges avec une carte à puce en utilisant le sous-système « lecteur de carte à puce Bull CP8 ».

Pré requis et préparation.

Cours sur les cartes à puces avec la présentation des éléments de la famille CP8 de Bull.

Cours sur la programmation en C d'un échange par liaison série.

Préparation.

Indiquer les éléments qui interviennent dans la mise en œuvre d'une carte de la famille CP8.

Indiquer le format d'une trame échangée entre le PC et le lecteur et l'encapsulation éventuelle du message échangé entre le lecteur et la carte.

On demande d'étudier les programmes sources fournis en annexe et permettant le pilotage du lecteur.

Activités.

A1 : connexion et commande du lecteur.

En utilisant les éléments fournis comme ressource et étudié en préparation, réaliser le programme permettant le dialogue avec lecteur et par conséquent la carte à puce insérée dans ce dernier.

Observer les trames échangées et indiquer les informations d'elles nous permettent de découvrir (test avec carte présente ou non). Commenter le rôle de chacun des octets en vous référant au Manuel d'utilisation SCOT de la page 96 à 99.

A2 : les paramètres de base d'une carte.

On demande de modifier le programme précédent afin de tester les fonctions de base ci-dessous pour lesquelles on fournit les informations relatives aux échanges :

RAZ ou ATR :
60 04 6E 01 00 00 0B $^{E}_{X}$

STX	60	Caractère de début de chaîne
LNG	04	Longueur de la trame
INS	6E	Provoque la mise sous tension de la carte.
P1	01	Temps d'attente d'instruction carte exprimé en seconde.
P2	00	Non significatif
P3	00	
LRC	0B	Checksum
ETX	$^{E}_{X}$	Caractère de fin de chaîne (0x03)

60 05 FB 18 00 00 0B 8D $^{E}_{X}$ -> carte absente

STX	60	Caractère de début de chaîne
LNG	05	Longueur de la trame
STATUS	FB	Status de carte absente.
P1	18	Type de coupleur.
P2	00	Non significatif
P3	00	
	0B	
LRC	8D	Checksum
ETX	$^{E}_{X}$	Caractère de fin de chaîne (0x03)

60 0F 00 18 02 0B C0 65 11 25 00 00 24 09 61 90 00 33 EX -> carte présente

STX	60	Caractère de début de chaîne
LNG	0F	Longueur de la trame
STATUS	00	La commande s'est correctement déroulée
P1	18	Type de coupleur.
P2	02	Type de carte (ici ISO 7816-3)
TS	C0	Nombre d'octets émis par la carte.
TO	65	Présence des octets système TB1, TC1 et de 5 octets caractérisant l'application.
TA1	11	Valeur par défaut défini par la norme.
TB1	25	VPP=5V (ici SCOT 50)
TC1	00	Intervalle maximal séparant l'émission par le lecteur de 2 octets (00 pour la famille SCOT 50
TD1	00	Valeur par défaut défini par la norme.
MCE	24	Identifie la carte (ici pour SCOT 50)
MCF	09	Identifie le système d'exploitation (09 pour la famille SCOT)
MCH	61	Renseigne sur l'état des verrous (donc la phase de vie de la carte) et le niveau de protection de la zone de travail.
SW1	90	Ordre exécuté
SW2	00	Fonctionnement normal de la carte
LRC	33	Checksum
ETX	EX	Caractère de fin de chaîne (0x03)

Lecture d'un mot à l'adresse 280 :
60 06 DB BC B0 02 80 04 37 EX

STX	60	Caractère de début de chaîne
LNG	06	Longueur de la trame
INS	DB	Ordre sortant
CLA	BC	Classe appelée
INS	B0	Ordre de lecture.
P1	02	Poid fort de l'adresse à la quelle on veut lire
P2	80	Poid faible de l'adresse à la quelle on veut lire
P3	04	Nombre d'octet que l'on veut lire
LRC	37	Checksum
ETX	EX	Caractère de fin de chaîne (0x03)

60 07 00 FF FF FF FF 90 00 F7 EX

STX	60	Caractère de début de chaîne
LNG	07	Longueur de la trame
INS	00	La commande s'est correctement déroulée
Données	FF	Mot contenu à l'adresse indiqué dans l'ordre de lecture (ici 280)
	FF	
	FF	
	FF	
SW1	90	Ordre exécuté
SW2	00	Fonctionnement normal de la carte
LRC	F7	Checksum
ETX	EX	Caractère de fin de chaîne (0x03)

Demande d'écriture du mot 12345678 à l'adresse 280 :
60 0A DA BC DO 02 80 12 34 56 78 52 EX
Réponse : ordre correctement exécuté :
60 03 00 90 00 F3 EX

Les trames en bleu correspondent aux trames reçues par le PC

Présentation du code porteur en format interne de la carte:
60 0A DA BC 20 00 00 04 12 54 3F FF AE EX
Réponse : ordre correctement exécuté :
60 03 00 90 00 F3 EX

Les trames en vert correspondent aux trames envoyées par le PC

Validation de code porteur :
60 06 DA BC 40 00 00 00 40 EX
Réponse : code valide :
60 03 00 90 00 F3 EX (si le code était mauvais il y aurait 14 à la place des 2 octets soulignés)

Effacement d'un mot à l'adresse 280 :
60 08 DA BC 0E 02 80 02 02 88 0A EX
Réponse : ordre correctement exécuté :
60 03 00 90 00 F3 EX

Enlever la carte :

60 01 4D 2C $^{E}_{X}$

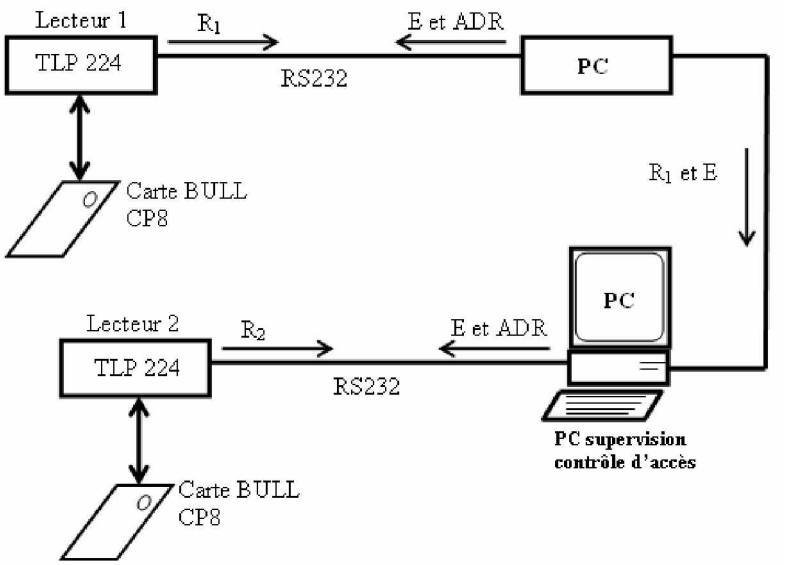
STX	60	Caractère de début de chaîne
P1	01	Temps d'attente d'instruction carte exprimé en seconde.
INS	4D	Provoque la mise hors tension de la carte.
LRC	2C	Checksum
ETX	$^{E}_{X}$	Caractère de fin de chaîne (0x03)

60 03 00 00 00 63 $^{E}_{X}$ -> carte toujours présente

60 03 F7 00 00 94 $^{E}_{X}$ -> carte enlevé

A3 : La fonction TELEPASS.

Cette fonction permet de valider une carte « esclave » en utilisant une carte « maître ». On calcule un certificat en utilisant les variables R1 et E sur les 2 cartes d'un même lot et on doit trouver la même « clé » calculée par chacune des cartes.



Calcul de certificat :

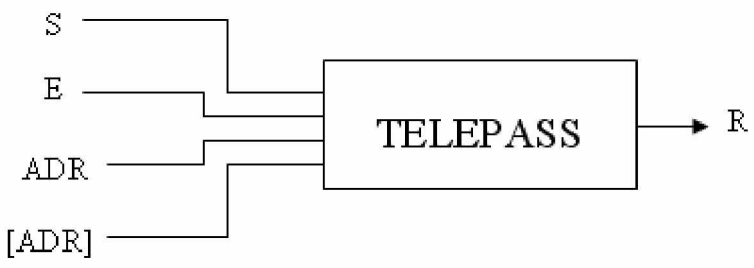
Pour faire le calcul de certificat on fournit deux valeurs à la carte à puce :

- un nombre aléatoire E sur 48 bits
- une adresse ADR sur 16 bits

La carte utilise également deux valeurs internes :

- le contenu de l'adresse (ADR) sur 32 bits
- un jeu secret S sur 96 bits (qui est le même pour un même lot de fabrication de cartes

Avec un algorithme de cryptage et les valeurs citées précédemment la carte va effectuer un calcul de certificat et renverra une réponse R sur 64 bits.



Contrôle de certificat :

1. Le PC1 va générer le nombre aléatoire E et envoyer E et l'adresse ADR (fixé par le programme) à la 1ère carte.
2. La 1ère carte renvoie à le résultat du calcul R_1
3. On envoie le résultat R_1 et le nombre E au PC de supervision
4. Le PC de supervision envoie le nombre E et l'adresse ADR à la 2ème carte.
5. La 2ème carte renvoie au PC de supervision le résultat du calcul R_2
6. Le PC de supervision va comparer R1 et R2 et si ils sont identiques les deux cartes viennent du même lot de fabrication.

Calcul de certificat TELEPASS :
Envoi d'un mot E et d'une adresse ADR :
60 0E DA BC 80 00 00 08 01 23 45 67 89 AB 02 80 20 EX
Réponse : ordre correctement exécuté :
60 03 00 90 00 F3 EX
Demande de lecture de résultat :
60 06 DB BC C0 00 00 08 C9 EX
Résultat renvoyé par la carte :
60 0B 00 35 7F 9C C7 19 51 22 5B 90 00 DB EX

On demande d'effectuer la demande de certificat pour 2 cartes et d'indiquer si elles appartiennent au même lot de fabrication.

A3 : Le code porteur d'une carte.

Grâce aux indications ci-dessous indiquer comment mettre en œuvre la notion de code porteur pour une carte.

Demande de déblocage de la carte :
Envoi du code porteur en format interne de la carte ainsi que la clé de déblocage 1A :
60 12 DA BC 20 00 00 0C 12 54 3F FF 23 45 67 89 23 45 67 89 BE EX
Réponse : la carte est bloquée :
60 03 E7 90 40 54 EX
Demande de validation en lecture :
60 06 DA BC 40 00 00 00 40 EX
Réponse : tout c'est correctement déroulé, la carte est débloquée :
60 03 00 90 00 F3 EX

Changer le code porteur 2A en code porteur 2B :
Demande d'écriture à l'adresse 250 du nouveau code porteur:
60 0A DA BC D0 02 50 04 05 80 7F FF 8F EX
Réponse : l'écriture c'est correctement déroulé:
60 03 00 90 00 F3 EX
Lecture d'un mot à l'adresse 250 :
60 06 DB BC B0 02 50 04 E7 EX
Réponse : l'écriture c'est correctement déroulé:
60 07 00 05 80 7F FF 90 00 F2 EX
Demande de validation en écriture :
60 06 DA BC 70 02 50 00 22 EX
Réponse : l'écriture c'est correctement déroulé:
60 03 00 90 00 F3 EX
Positionnement du verrou LU :
60 08 DA BC 50 00 00 02 7F FF DC EX
Réponse : le verrou a été posé correctement :
60 03 00 90 00 F3 EX

Compte rendu

Présenter sous forme d'un diaporama :

- Les fonctions disponibles pour la carte SCOT 50 de la famille Bull CP8.
- La mise en œuvre de ces fonctions.