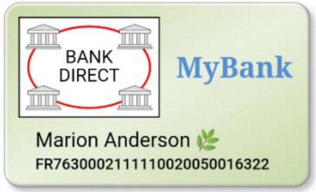
Saturn V3 - Payment Credentials

Name	Comment	Example/Implementation
paymentMethod	URI indicating payment method.	*Fictitious bank driven payment network:* **https://bankdirect.net**
accountId	Account identifier associated with the payment credential.	*Fictitious French IBAN account:* **FR7630002111110020050016322**
providerAuthorityUrl	Points to the issuer. Used for gathering information about methods and service end points. *This data also plays a crucial role for establishing scalable trust between entities*.	*Fictitious bank URL:* **https://pay.mybank.com/authority** See: https://cyberphone.github.io/doc/defensive-publications/authority-objects.pdf
encryptionParameters	Holds an object with parameters (*including a bank specific public key*), telling the local client application how to encrypt user authorization data (an alternative to "tokenization").	Object based on IETF's JOSE standards: • EC or RSA public key in JWK format • Content encryption algorithms like A256GCM • Key encryption algorithms like ECDH-ES
authorizationKey	Private key (including public key) used for authorizing payment requests associated with **accountId**. *This key must be explicitly activated by the user through a PIN code or biometric operation*.	Generated and stored in a TEE. *Only the corresponding public key is ever transmitted in clear.*
accountBalanceKey	Private key (including public key) used for authorizing balance requests associated with **accountId**. *This key is used in the background and does not require user interaction since balance access is read only and limited to a specific account*.	Generated and stored in a TEE. *Only the corresponding public key is ever transmitted in clear.*
imageData	SVG image holding a visual representation of the payment credential.	 BANK DIRECT MyBank Marion Anderson FR7630002111110020050016322

V0.8, A.Rundgren 2019-08-12