

Saturn V3 - Payment Credentials

Name	Comment	Example/Implementation
paymentMethod	URI indicating payment method.	<i>Fictitious bank driven payment network:</i> https://bankdirect.net
accountId	Account identifier associated with the credential.	<i>Fictitious French IBAN account:</i> FR7630002111110020050016322
providerAuthorityUrl	Points to the issuer. Used for gathering information about methods and service end points. <i>This data also plays a crucial role for establishing scalable trust between entities.</i>	<i>Fictitious bank URL:</i> https://pay.mybank.com/authority See: https://cyberphone.github.io/doc/defensive-publications/authority-objects.pdf
encryptionParameters	Holds an object with parameters (<i>including a bank specific public key</i>), telling the local client application how to encrypt user authorization data (an alternative to “tokenization”).	Object based on IETF’s JOSE standards: <ul style="list-style-type: none"> • 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. <i>This key must be explicitly activated by the user through a PIN code or biometric operation.</i>	Generated and stored in a TEE. <i>Only the corresponding public key is ever transmitted in clear.</i>
accountBalanceKey	Private key (including public key) used for authorizing balance requests associated with accountId. <i>This key is used in the background and does not require user interaction since it only reads data and only for a specific account.</i>	Generated and stored in a TEE. <i>Only the corresponding public key is ever transmitted in clear.</i>
imageData	SVG image holding a visual representation of the credential.	