Cryptocurrency Wallet Security Requirements Checklist

Domain	Category	Security Requirement	Impacted Node	Removed Node
Common	Authentication	a. Does the wallet hide the PIN or password on the screen?	T3(AC), T55(AC), T76(AC), T103(AC), T127(AC)	
		b. Does the wallet get disabled after a certain amount of consecutive unsuccessful authentication attempts?	T5(AC), T57(AC), T78(AC), T105(AC), T129(AC)	
		c. Does the wallet get locked if it is not used for a certain period of time?	T4(AC), T56(AC), T77(AC), T104(AC), T128(AC)	
		d. Can passphrase be added to the recovery phrase to create a hidden wallet?		T10(X), T110(X)
		e. Is there any protection mechanism for authentication credentials (e.g., encryption, hash, or secure element)?		T8(X), T60(X), T81(X), T108(X), T132(X)
		f. Is there any defense mechanism for physical attacks (e.g., fault injection) on the user authentication process?	T9(AC), T61(AC), T82(AC), T109(AC), T133(AC)	
	Output	a. Is there a mechanism to prevent screen capture when a private key or recovery phrase is displayed?	T12(AC)	
		b. Does the wallet deliver a warning message about the risk of exposing a private key or recovery phrase before they are displayed?	T11(AC)	
		c. Is user authentication required before displaying a private key or recovery phrase at the request of a user?		B5(X)
	Input	a. Is there a defense mechanism for keylogging attacks when a private key or recovery phrase is entered by a user?	T1(AC)	
	Copy	a. Is it forbidden to copy a private key or recovery phrase to the clipboard?		B13(O)
	Key Generation	a. Is a proven random number generator used to generate a seed or a private key?	T39(TC)	
		b. Is more than 112-bit entropy used to generate a master seed?	T39(TC)	
	Key Management	a. Is an encryption key that provides more than 112 bits of security length used to encrypt a private key or recovery phrase?	T18(TC)	
		b. Is there an access control mechanism for the encrypted private key or recovery phrase?		T17(X)
		c. Is there any defense mechanism for physical attacks (e.g., microprobing or reverse engineering)on the device?	T14(AC), T19(AC), T23(AC), T34(AC), T46(AC), T72(AC)	
	Transaction	a. Is the detail of a new transaction displayed and user confirmation is required before signing the transaction?	T53(AC)	
		b. Is user authentication required before signing a new transaction?		B35(X)
		c. Is a proven random number generator used to generate a signature?	T37(TC), T38(TC)	
	Application	a. Is there any integrity verification mechanism for the wallet application or wallet manager?	T29(AC), T30(AC), T41(AC), T42(AC), T70(AC), T71(AC)	
	Network	a. Is data transmitted across networks through secure channels (e.g., HTTPS)?	T98(AC), T99(AC), T100(AC), T138(AC), T139(AC), T140(AC), T141(AC)	
		b. Does the wallet device keep offline (air-gapped) when it is not used?	T1(AV, AC), T12(AV, AC), T15(AV, AC), T22(AV, AC), T26(AV, AC), T27(AV, AC), T49(AV, AC), T52(AV, AC), T65(AV, AC), T87(AV, AC), T90(AV, AC), T95(AV, AC), T97(AV, AC), T111(AV, AC), T112(AV, AC), T113(AV, AC), T114(AV, AC), T121(AV, AC), T125(AV, AC), T134(AV, AC), T135(AV, AC), T136(AV, AC), T138(AV, AC)	
	Recovery	a. Are there any instructions explaining the importance of	S4(A), S5(A)	

		backing up private keys or a recovery phrase?		
		b. Is there a mechanism to check if the user has backed up a private key or recovery phrase?	S4(A), S5(A)	
	Privacy	a. Is personally identifiable user information (e.g., name, email address, or phone number) is not entered or stored in the wallet?		S8(O)
		b. Is user authentication required before displaying an account address or balance?		B63(X)
Embedded System	Output	a. Is there an output interface to display an account address or transaction information for user confirmation?	T53(AC)	T13(O), T116(O)
	Firmware	a. Is there any firmware integrity verification mechanism?	T32(AC), T33(AC), T44(AC), T45(AC), T67(AC), T68(AC)	
	Debugger	a. Are debugger pins removed or disabled (e.g., JTAG interface)?		
	Communication	a. Is there a secure communication mechanism between the host and the wallet device (e.g., secure channel)?	T137(TC)	
	Authentication	a. Is there a mechanism for checking the authenticity of the wallet device that is connected to the host?	T35(AC), T36(AC), T47(AC), T48(AC), T73(AC), T74(AC),	
	Authorization	a. Is there an authorization mechanism for the wallet manager that is installed on the external host?	T53(AC)	
Mobile	Privilege Escalation	a. Is there a mechanism to check if the device is rooted?	T22(AC), T26(AC), T52(AC), T65(AC), T87(AC),T95(AC), T121(AC), T125(AC)	

Cryptocurrency Wallet Security Requirements Checklist (Omitted Version)

Domain	Category	Security Requirement	Impacted Node	Removed Node
Common	Authentication	a. Does the wallet hide the PIN or password on the screen?	T3(AC), T55(AC), T76(AC), T103(AC), T127(AC)	
		b. Does the wallet get disabled after a certain amount of consecutive unsuccessful authentication attempts?	T5(AC), T57(AC), T78(AC), T105(AC), T129(AC)	
	Output	a. Is there a mechanism to prevent screen capture when a private key or recovery phrase is displayed?	T12(AC)	
	Input	a. Is there a defense mechanism for keylogging attacks when a private key or recovery phrase is entered by a user?	T1(AC)	
	Copy	a. Is it forbidden to copy a private key or recovery phrase to the clipboard?		B13(O)
	Key Generation	a. Is a proven random number generator used to generate a seed or a private key?	T39(TC)	
	Key Management	a. Is an encryption key that provides more than 112 bits of security length used to encrypt a private key or recovery phrase?	T18(TC)	
	Transaction	a. Is the detail of a new transaction displayed and user confirmation is required before signing the transaction?	T53(AC)	
	Application	a. Is there any integrity verification mechanism for the wallet application or wallet manager?	T29(AC), T30(AC), T41(AC), T42(AC), T70(AC), T71(AC)	
	Network	b. Does the wallet device keep offline (air-gapped) when it is not used?	T1(AV, AC), T12(AV, AC), T15(AV, AC), T22(AV, AC), … , T136(AV, AC), T138(AV, AC)	
	Recovery	a. Are there any instructions explaining the importance of backing up private keys or a recovery phrase?	S4(A), S5(A)	
	Privacy	a. Is personally identifiable user information (e.g., name, email address, or phone number) is not entered or stored in the wallet?		S8(O)
Embedded System	Output	a. Is there an output interface to display an account address or transaction information for user confirmation?	T53(AC)	
	Firmware	a. Is there any firmware integrity verification mechanism?	T32(AC), T33(AC), T44(AC), T45(AC), T67(AC), T68(AC)	
	Debugger	a. Are debugger pins removed or disabled (e.g., JTAG interface)?		T13(O), T116(O)
	Communication	a. Is there a secure communication mechanism between the host and the wallet device (e.g., secure channel)?	T137(TC)	
	Authentication	a. Is there a mechanism for checking the authenticity of the wallet device that is connected to the host?	T35(AC), T36(AC), T47(AC), T48(AC), T73(AC), T74(AC),	
	Authorization	a. Is there an authorization mechanism for the wallet manager that is installed on the external host?	T53(AC)	
Mobile	Privilege Escalation	a. Is there a mechanism to check if the device is rooted?	T22(AC), T26(AC), T52(AC), T65(AC), T87(AC),T95(AC), T121(AC), T125(AC)	

Cryptocurrency Wallet Security Requirements Analysis Result

Domain	Category	Security Requirement	Ledger Nano S	Trezor One	Bread Wallet	Trust Wallet	Copay Wallet	Electrum Wallet
Common	Authentication	a. Does the wallet hide the PIN or password on the screen?	△	O	O	O	O	O
		b. Does the wallet get disabled after a certain amount of consecutive unsuccessful authentication attempts?	O	O	△	O	X	X
		c. Does the wallet get locked if it is not used for a certain period of time?	O	X	X	O	X	X
		d. Can passphrase be added to the recovery phrase to create a hidden wallet?	O	O	X	X	X	X
		e. Is there any protection mechanism for authentication credentials (e.g., encryption, hash, or secure element)?	O	O	O	O	O	O
		f. Is there any defense mechanism for physical attacks (e.g., fault injection) on the user authentication process?	O	X	X	X	X	X
	Output	a. Is there a mechanism to prevent screen capture when a private key or recovery phrase is displayed?	O	O	X	O	X	X
		b. Does the wallet deliver a warning message about the risk of exposing a private key or recovery phrase before they are displayed?	X	O	X	O	O	O
		c. Is user authentication required before displaying a private key or recovery phrase at the request of a user?	O	O	O	O	O	O
	Input	a. Is there a defense mechanism for keylogging attacks when a private key or recovery phrase is entered by a user?	O	O	X	X	X	X
	Copy	a. Is it forbidden to copy a private key or recovery phrase to the clipboard?	O	O	X	O	X	X
	Key Generation	a. Is a proven random number generator used to generate a seed or a private key?	O	O	O	O	O	O
		b. Is more than 112-bit entropy used to generate a master seed?	O	O	O	O	O	O
	Key Management	a. Is an encryption key that provides more than 112 bits of security length used to encrypt a private key or recovery phrase?	O	O	O	O	O	O
		b. Is there an access control mechanism for the encrypted private key or recovery phrase?	O	O	O	O	X	X
		c. Is there any defense mechanism for physical attacks (e.g., microprobing or reverse engineering)on the device?	O	X	X	X	X	X
	Transaction	a. Is the detail of a new transaction displayed and user confirmation is required before signing the transaction?	O	O	O	O	O	O
		b. Is user authentication required before signing a new transaction?	O	O	O	O	O	O
		c. Is a proven random number generator used to generate a signature?	O	O	O	O	O	O
	Application	a. Is there any integrity verification mechanism for the wallet application or wallet manager?	O	O	O	O	O	O
	Network	a. Is data transmitted across networks through secure channels (e.g., HTTPS)?	O	O	O	O	O	O
		b. Does the wallet device keep offline (air-gapped) when it is not used?	O	O	X	X	X	X
	Recovery	a. Are there any instructions explaining the importance of backing up private keys or a recovery phrase?	O	O	△	O	O	O
		b. Is there a mechanism to check if the user has backed up a private key or recovery phrase?	O	X	O	O	O	O
	Privacy	a. Is personally identifiable user information (e.g., name, email address, or phone number) is not entered or stored in the wallet?	O	O	O	O	△	O
		b. Is user authentication required before displaying an account address or balance?	O	O	O	O	X	O

Embedded System	Output	a. Is there an output interface to display an account address or transaction information for user confirmation?	O	O	-	-	-	-
	Firmware	a. Is there any firmware integrity verification mechanism?	O	O	-	-	-	-
	Debugger	a. Are debugger pins removed or disabled (e.g., JTAG interface)?	O	O	-	-	-	-
	Communication	a. Is there a secure communication mechanism between the host and the wallet device (e.g., secure channel)?	O	X	-	-	-	-
	Authentication	a. Is there a mechanism for checking the authenticity of the wallet device that is connected to the host?	O	X	-	-	-	-
	Authorization	a. Is there an authorization mechanism for the wallet manager that is installed on the external host?	O	O	-	-	-	-
Mobile	Privilege Escalation	a. Is there a mechanism to check if the device is rooted?	-	-	O	O	-	-

Cryptocurrency Wallet Security Requirements Analysis Result (Omitted Version)

Domain	Category	Security Requirement	Ledger Nano S	Trezor One	Bread Wallet	Trust Wallet	Copay Wallet	Electrum Wallet
Common	Authentication	a. Does the wallet hide the PIN or password on the screen?	△	O	O	O	O	O
		b. Does the wallet get disabled after a certain amount of consecutive unsuccessful authentication attempts?	O	O	△	O	X	X
	Output	a. Is there a mechanism to prevent screen capture when a private key or recovery phrase is displayed?	O	O	X	O	X	X
	Input	a. Is there a defense mechanism for keylogging attacks when a private key or recovery phrase is entered by a user?	O	O	X	X	X	X
	Copy	a. Is it forbidden to copy a private key or recovery phrase to the clipboard?	O	O	X	O	X	X
	Key Generation	a. Is a proven random number generator used to generate a seed or a private key?	O	O	O	O	O	O
	Key Management	a. Is an encryption key that provides more than 112 bits of security length used to encrypt a private key or recovery phrase?	O	O	O	O	O	O
	Transaction	a. Is the detail of a new transaction displayed and user confirmation is required before signing the transaction?	O	O	O	O	O	O
	Application	a. Is there any integrity verification mechanism for the wallet application or wallet manager?	O	O	O	O	O	O
	Network	b. Does the wallet device keep offline (air-gapped) when it is not used?	O	O	X	X	X	X
	Recovery	a. Are there any instructions explaining the importance of backing up private keys or a recovery phrase?	O	O	△	O	O	O
	Privacy	a. Is personally identifiable user information (e.g., name, email address, or phone number) is not entered or stored in the wallet?	O	O	O	O	△	O
Embedded System	Output	a. Is there an output interface to display an account address or transaction information for user confirmation?	O	O	-	-	-	-
	Firmware	a. Is there any firmware integrity verification mechanism?	O	O	-	-	-	-
	Debugger	a. Are debugger pins removed or disabled (e.g., JTAG interface)?	O	O	-	-	-	-
	Communication	a. Is there a secure communication mechanism between the host and the wallet device (e.g., secure channel)?	O	X	-	-	-	-
	Authentication	a. Is there a mechanism for checking the authenticity of the wallet device that is connected to the host?	O	X	-	-	-	-
	Authorization	a. Is there an authorization mechanism for the wallet manager that is installed on the external host?	O	O	-	-	-	-
Mobile	Privilege Escalation	a. Is there a mechanism to check if the device is rooted?	-	-	O	O	-	-