Concept 731: AP Crypto Rework

Final release planned for R25-11

Till Neudecker

03 Feb 2025

AP Crypto Rework

Final release planned for R25-11

Challenge	Solution
The current ara::crypto API makes usage unnecessarily complex for the user. • E.g., abstractions (“IoInterface”), redundant ways of achieving the same result (e.g., persisting a key)	Simplify the use of ara::crypto by removing unnecessary abstractions and features.
The current ara::crypto API restricts stack implementations by specifying implementation details.	Reduce the specification to the definition of the user-interfaces. All stack internal interfaces (e.g., “KeyStorageProvider”) are removed.
The continuous changes since introduction of ara::crypto lead to many inconsistencies in the ara::crypto specification.	Specify a consistent state that incorporates the lessons learned from real-world project experiences since 2019.

Simpler and more robust use of ara::crypto