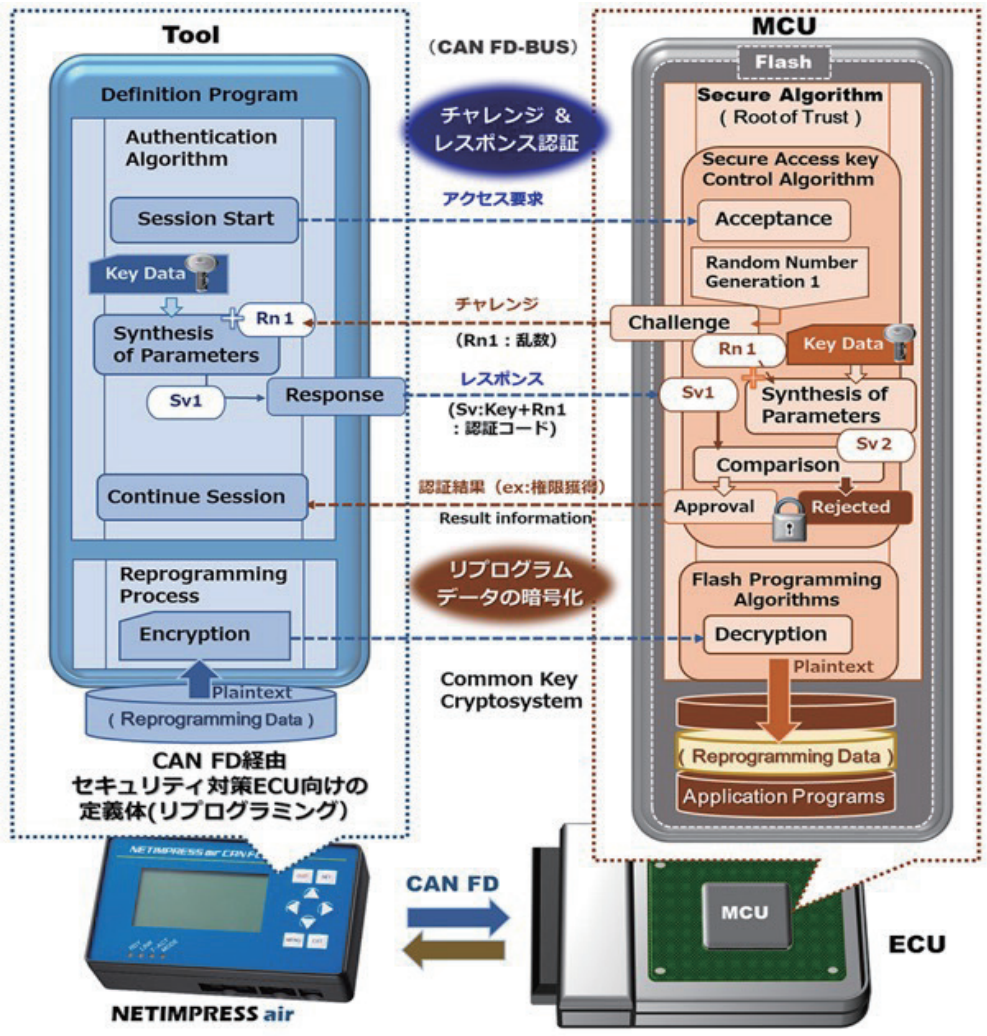
CASE時代に変化する車載ネットワークセキュリティ要件に追従

OEM車両に準じた ECUリプログラミングの認証・暗号化対応

NETIMPRESS airは、各種ECU診断プロトコルに実装されたセキュリティ対策の認証アルゴリズムをインテグレーションが可能で、診断のリプログラミング機能に準じたプログラミングツールを提供

OEM車両に準じたセキュリティ対策の認証と暗号化の例：カスタムの対応可能



ECUソフトウェア更新対応の車載セキュリティ対策（認証・コード暗号化）

車両ネットワーク上の不正アクセス・盗聴、なりすましによるECUの改ざん、マルウェアの混入などの防止

●アクセス要求

リプログラムのセッション開始としてツール側からECUへ認証要求を行う。（ECUとツール間で共有された鍵情報（Key Data）を相互で保有する。）

●チャレンジ

ツール側からの要求を受付後、チャレンジデータ用に乱数を生成し、その乱数値（Rn1）をツール側に送信。

●レスポンス

ECU側からの受信データ（乱数値）とツールが保有している鍵情報の二つのパラメータを暗号化のための合成を行う。（暗号化にはハッシュ関数の利用がある）合成した値（Sv1）を認証コードとしてECU側へ送信する。

●レスポンス判定

チャレンジデータ（Rn1）とECUが保有している鍵情報の二つのパラメータを暗号化のための合成を行い、レスポンスの比較用の値（Sv2）を生成する。ツール側から受信した認証コード（Sv1）と、ECUで生成した比較用データ（Sv2）の照合判定を行う。

●開通承認

照合判定の結果が正しければアクセス権限を獲得し、開通承認の結果をツールへ通知する。ツールとECUのセッションが継続される。誤りの場合は認証が無効であることを通知し、セッションが中断される。

生産ライン向けフラッシュ書き込みソリューション

汎用・高速オンボードプログラマ　NETIMPRESSシリーズ

NETIMPRESS avant

NETIMPRESS acorde

自動プログラミングシステム

APX1000
NEW

DTS インサイト

Our insight, your value