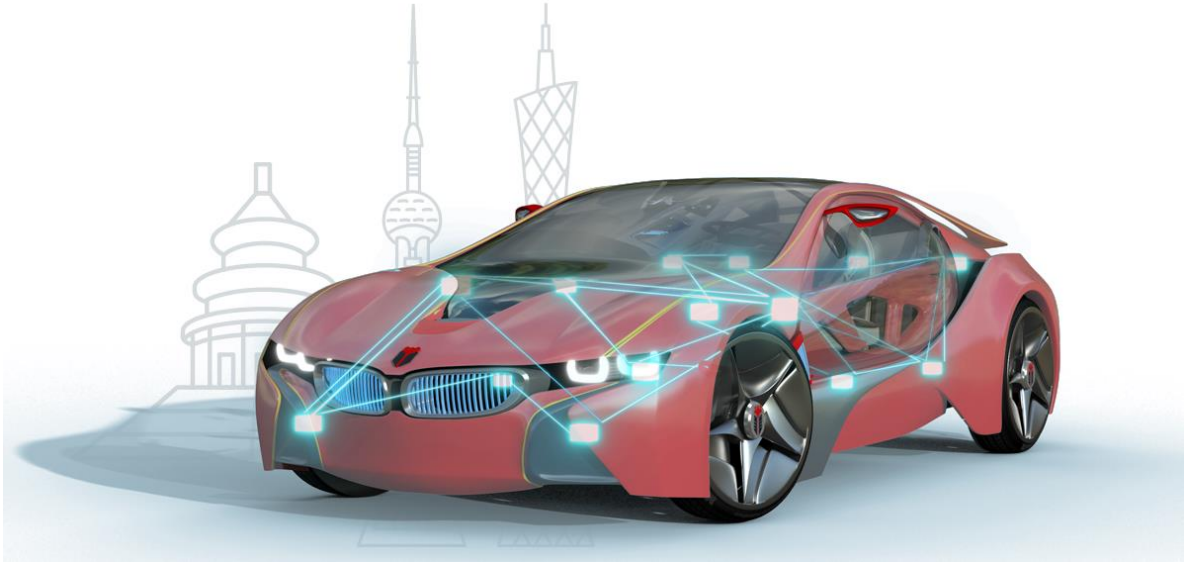
知从玄武信息安全功能介绍

ZC.XUANWU CYBERSECURITY INTRODUCTION

知从玄武工具

ZC.XuanWu Tool



知从玄武信息安全功能

ZC.XUANWU CYBERSECURITY INTRODUCTION

知从玄武工具

ZC.XuanWu Tool

1 概述 OVERVIEW

玄武上位机软件用来将电子控制器中的应用程序和数据，从 PC 端下载到电子控制器上。支持UDSonCAN、UDSonEth、UDSonK-Line、UDSonLIN协议。提供客户协议定制集成，广泛应用在电子控制器产品开发阶段，测试阶段，售后服务阶段。

ZC.XuanWu upper computer software is used to download application programs and data from the PC to the electronic controller. It supports UDS on CAN, UDS on Eth, UDS on K-Line, and UDS on LIN protocols. It offers customized integration of customer-specific protocols and is widely used in the development, testing, and after-sales service stages of electronic controller products.

知从玄武程序刷新与诊断测试工具可应用于 OEM 和 Tier1 多种应用场景下。用户可以方便的在实验室，试验车辆以及实车上方便的进行程序刷写工作。

ZC.XuanWu program refresh and diagnostic testing tools can be applied in various application scenarios for OEMs and Tier 1 suppliers. Users can conveniently perform program flashing work in laboratories, test vehicles, and actual vehicles.

玄武上位机软件目前应用于各类电子控制器的程序刷写：

ZC.XuanWu upper computer software is currently used for program flashing of various electronic controllers:

- 车身控制器 Body Control Module (BCM)
- 空调控制器 Air Conditioning Controller
- DC/DC 控制器 DC/DC Converter

- 电子助力转向控制器 Electric Power Steering Controller
- 发动机控制器 Engine Management System (EMS)
- 变速箱控制器 Transmission Control Module (TCM)
- 电池管理系统 Battery Management System (BMS)
- 整车控制器 Vehicle Control Unit (VCU)
- 电机控制器 Motor Control Unit (MCU)
- 电动助力转向系统 Electric Power Steering System (EPS)
- 防抱死制动系统 Anti-lock Braking System (ABS)
- 电子稳定性控制程序 Electronic Stability Program (ESP)
- 主动防撞系统 Active Collision Avoidance System (ACC)
- 牵引力控制系统 Traction Control System (TCS)
- ADAS 控制器 Advanced Driver Assistance Systems Controller

配置环境 Configuration Environment	
Hardware	PCAN 、 Mongoose 、 Kvaser 、 USBCAN （ ZLG ） 、 VN1640 、 TC1016、OBD-RJ45
Configuration Environment	Win7/10 64bit

PCAN

Mongoose

USBCAN（ZLG）

Kvaser

VN1640

OBD-RJ45

TC1016

2 网络安全介绍 CYBERSECURITY INTRODUCTION

随着汽车新四化（尤其是网联化与自动驾驶）的推进，人们对汽车与多设备联网的需求日益提升 —— 这种联网不仅能大幅提升汽车安全与交通安全、促进绿色发展，还能带动信息互通。具体来看，车内设备不仅要与手机等智能设备连接，还需便捷接入互联网，与交通管理系统、周边车辆实现信息共享。与之相对应的是，汽车网络信息安全的重要性愈发凸显。

此外，随着车辆网联化、智能化进程的深化，云计算与大数据技术的应用普及，以及高级驾驶辅助系统（ADAS）的广泛落地，保障汽车网络信息安全已成为新一代汽车发展的必然选择。

With the advancement of automotive new four modernizations (particularly connectivity and autonomous driving), there is a growing demand for vehicles to connect with multiple devices. Such connectivity can significantly enhance automotive and traffic safety, promote green development, and facilitate information exchange. Specifically, in-vehicle devices need not only to connect with smart devices like smartphones but also to seamlessly access the internet, enabling data sharing with traffic management systems and surrounding vehicles. Correspondingly, the importance of automotive cybersecurity has become increasingly prominent.

Furthermore, as vehicle connectivity and intelligence deepen, alongside the widespread adoption of cloud computing, big data technologies, and the extensive deployment of Advanced Driver Assistance Systems (ADAS), ensuring automotive cybersecurity has become an inevitable requirement for the development of next-generation vehicles.

随着网络安全的风险日益加大，一旦出现干扰车辆制动、加速和转向系统的黑客行为就可能造成严重的后果。汽车网络安全作为网络信息的保护技术应运而生，它基于密码学基础，通过使用对称加密或非对称加密算法来对信息进行保护，能够大幅度降低网络信息泄露、被篡改的风险。

As cybersecurity risks continue to escalate, malicious interference with vehicle systems—such as braking, acceleration, and steering—could lead to severe consequences. In response, automotive cybersecurity has emerged as a critical protective technology for networked information. Rooted in cryptography, it employs symmetric or asymmetric encryption algorithms to safeguard data, significantly reducing the risks of information leaks and tampering.

汽车软件主流的安全机制有如下几种:

The mainstream security mechanisms in automotive software include the following:

- 安全启动(SecureBoot)
- 安全升级(SecureUpdate)
- 安全诊断(SecureDiagnostic)
- 安全存储(SecureStorage)
- 安全通信(SecOC)
- 安全日志(SecureLog)
- 安全调试(SecureDebug)

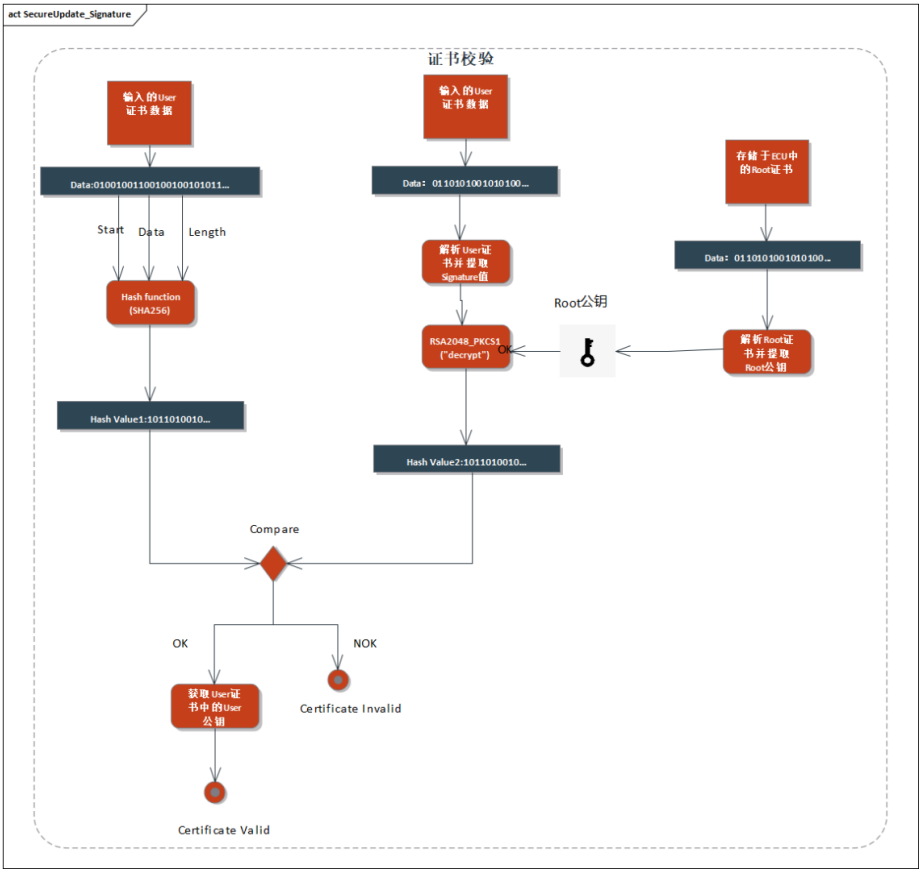
与刷写诊断相关的安全机制有以下两种：

The security mechanisms related to flashing and diagnostics mainly include the following two types:

2.1 安全升级 SecureUpdate

安全升级是为了确保待安装软件的真实性。通过对 FLASH 数据执行签名验证（支持 RSA /ECDSA 非对称算法及 SHA 哈希等对称加密算法）以验证代码的真实性，当且仅当签名验证成功时，ECU 才会方允许编程新固件至 FLASH，防止将设备降级更新到包含已知安全漏洞的旧版本软件，实现端到端代码真实性保护，抵御未授权篡改软件。

Secure updates are implemented to guarantee the authenticity of software to be installed. By performing signature verification on FLASH data (supporting asymmetric algorithms like RSA /ECDSA and symmetric encryption such as SHA hashing), the system validates the code's authenticity. The ECU will only permit programming new firmware into FLASH when the signature verification is successful. This prevents downgrading devices to older software versions containing known security vulnerabilities, thereby achieving end-to-end code authenticity protection and defending against unauthorized software tampering.



2.2 安全诊断 SecureDiagnostic

安全诊断通过某种认证算法来确认客户端的身份，从而决定客户端是否允许访问。基于 UDS 诊断协议，通过 UDS 0x27 服务，通过对称加密、非对称加密算法，依据随机数种子动态生成认证凭证来确定客户端身份。其次还可通过 UDS 0x29 服务，基于 ISO14229-1:2020 标准，通过支持以下两种安全概念：

Security diagnosis confirms the identity of the client through a certain authentication algorithm, thereby determining whether the client is allowed access. Based on the UDS diagnostic protocol, through the UDS 0x27 service, symmetric encryption and asymmetric encryption algorithms are used to dynamically generate authentication credentials based on random number seeds to determine the client's identity. Secondly, it can also be supported through the UDS 0x29 service based on the ISO14229-1:2020 standard by supporting the following two security concepts:

- 基于使用非对称密码的 PKI 证书交换过程。

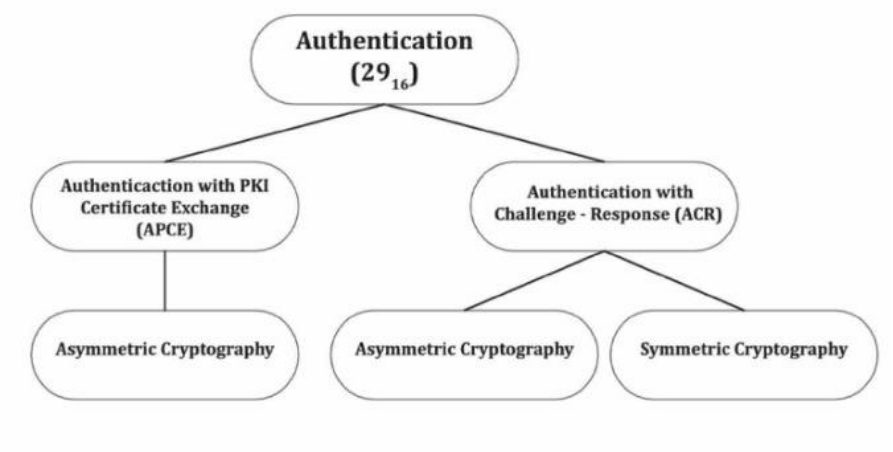
The PKI certificate exchange process based on the use of asymmetric cryptography.

- 基于不带 PKI 证书的挑战 - 应答过程，使用带有软件身份验证令牌或对称密码的非对称加密算法。

Based on a challenge-response process without PKI certificates, asymmetric encryption algorithms with software authentication tokens or symmetric passwords are used.

实现基于 0x29 服务中的各项子服务实现证书传递，签名、验签等来认证确认客户端身份，保障诊断接口安全，阻止客户端未经授权就访问敏感数据。

Implement certificate transmission, signature, signature verification, etc. based on various sub-services in the 0x29 service to authenticate and confirm the client's identity, ensure the security of the diagnostic interface, and prevent the client from accessing sensitive data without authorization.

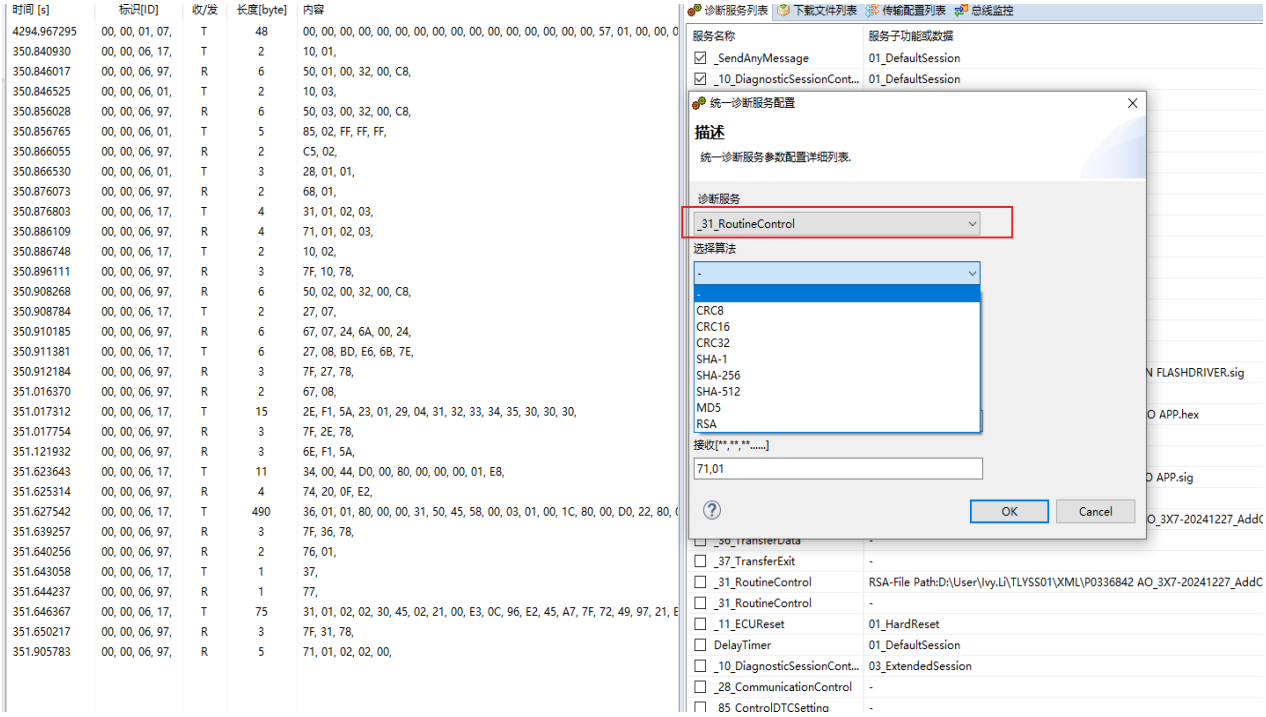


子服务 Sub-service	名称 Name	描述 Description
00	deAuthenticate	此子服务有效地结束认证状态。 This sub-service effectively ends the authentication state.
01	verifyCertificateUnidirectional	此子服务启动单向身份认证验证过程。 This sub-service initiates a unidirectional identity authentication process.
02	verifyCertificateBidirectional	此子服务启动双向身份认证验证过程。 This sub-service initiates a bidirectional identity authentication process.
03	proofOfOwnership	此子服务用于将所有权证明数据传输到诊断仪。 This sub-service is used to transmit proof of ownership data to the diagnostic tool.
04	transmitCertificate	此子服务用于证书或证书链传输。 This sub-service is used for the transmission of certificates or certificate chains.
08	authenticationConfiguration	此子服务用于显示 Server 所提供的认证配置 This sub-service is used to display the authentication configuration provided by the Server.

3.1 安全升级配置 SecureUpdate

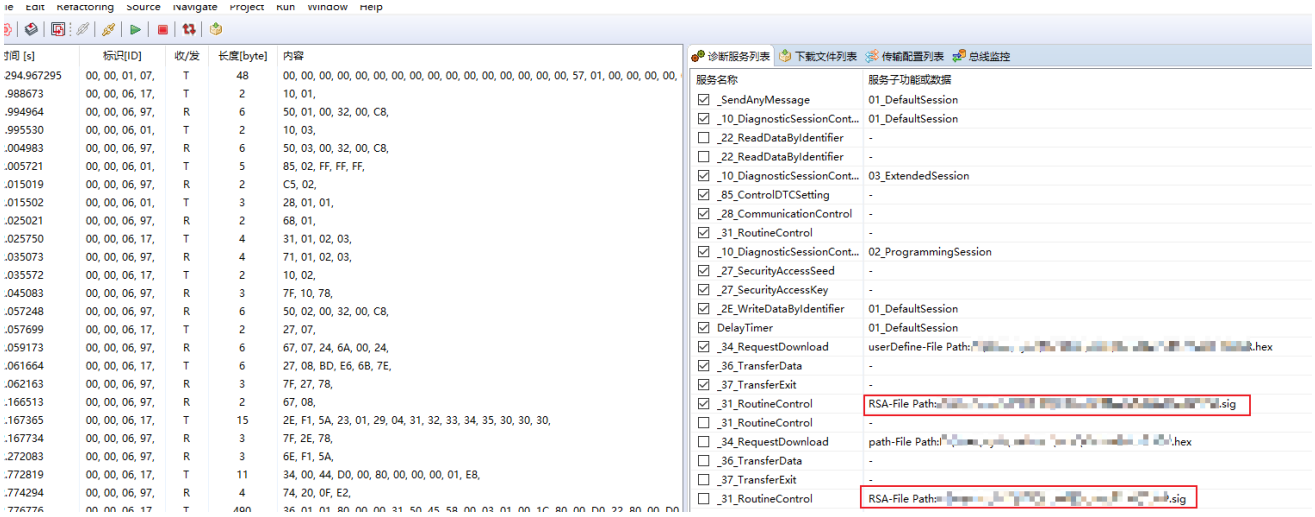
玄武支持用户向 ECU 发送单条或多条诊断报文，针对安全升级，玄武支持在新建 UDS 0x31 服务时进行配置，可以选择签名算法，如 RSA 等非对称加密算法、SHA 等对称加密算法，从而依据不同算法对于 FLASH 文件进行签名验证，以验证代码的真实性

Xuanwu enables users to send single or multiple diagnostic messages to the ECU. For security upgrades, Xuanwu supports configuration when creating a new UDS 0x31 service. Users can choose signature algorithms, such as asymmetric encryption algorithms like RSA and symmetric encryption algorithms like SHA, to verify the authenticity of the code by signing FLASH files based on different algorithms



玄武也支持手动选择.rsa /.sig 签名文件进行传输及验签：

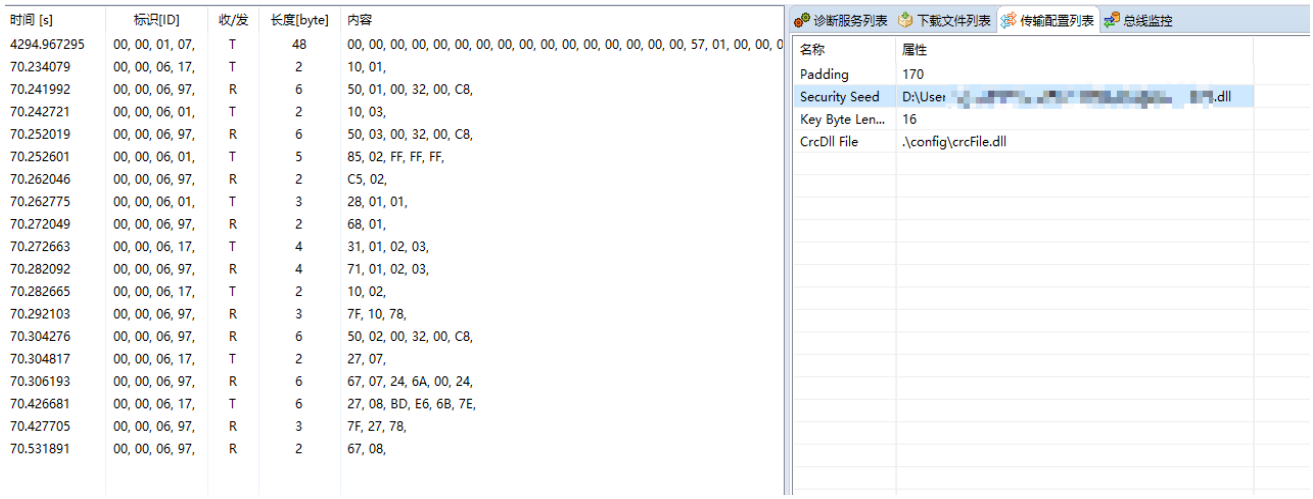
Xuanwu also supports manual selection of.rsa /.sig signed files for transmission and verification:



3.2 安全诊断配置 SecureDiagnostic

针对 0x27 服务，玄武可配置 Dll 路径，调用 Dll 实现多种算法去计算 key 值，支持多种算法，如：AES-CBC/AES-CMAC 算法、RSA 算法、HASH 算法

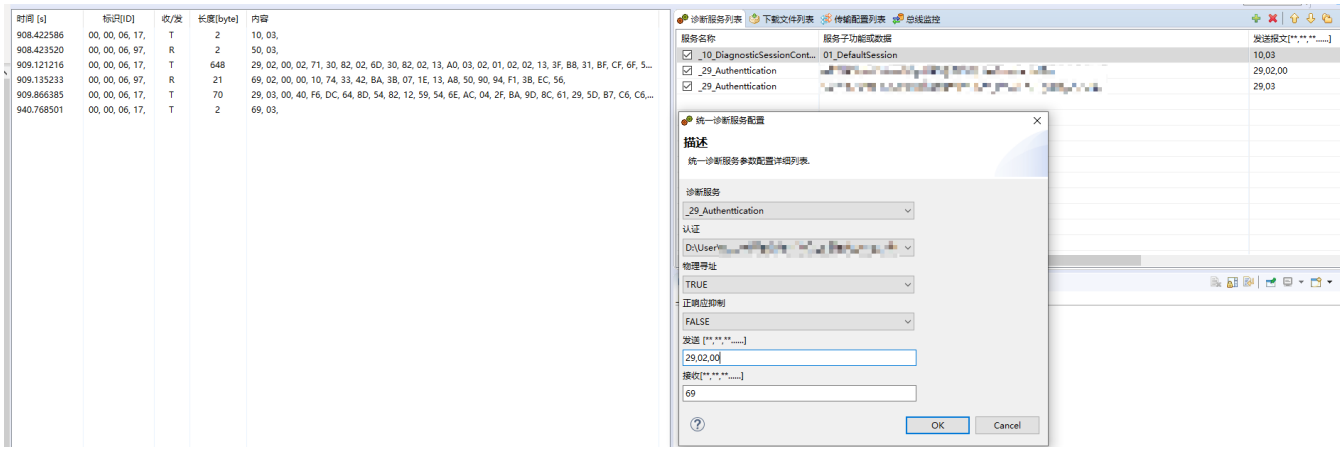
For the 0x27 service, Xuanwu can configure the Dll path and call the Dll to implement multiple algorithms to calculate the key value. It supports multiple algorithms, such as: AES-CBC/AES-CMAC algorithm, RSA algorithm, and HASH algorithm



针对 0x29 服务，玄武支持 29 服务证书传递，验签，签名等多种功能，可通过 29 01/02 等服务实现对于 ECU 的单向认证或双向认证。只需添加 29 01/02 服务时配置需传递证书文件，添加 29 03 服务时配置签名所用私钥证书文件，即可实现上述功能。

For the 0x29 service, Xuanwu supports multiple functions such as certificate transmission, signature verification, and signature for the 29 service. One-way or two-way authentication of the ECU can be achieved through services like 29 01/02. The above function can be achieved

simply by configuring the certificate file to be passed when adding the 29 01/02 service and configuring the private key certificate file used for signing when adding the 29 03 service.



4 证书 CERTIFICATE

中华人民共和国国家版权局
计算机软件著作权登记证书

证书号： 软著登字第13953481号

软 件 名 称： 知从玄武软件
[简称：知从玄武]
V10.1.0

著 作 权 人： 上海知从科技有限公司

权利取得方式： 原始取得

权 利 范 围： 全部权利

登 记 号： 2024SR1549608

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局
计算机软件著作权登记专用章

2024年10月17日

玄武软件著作权登记证书
XUANWU SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE