intertrust®

Building trust into connected cars

The Intertrust® solution to software threats in the automotive industry

Automotive industry under attack

The increasing number of smart features built into cars is inevitably leading to a serious potential threat—remote software attacks. Because connected cars are linked with the internet and its crucial systems are interconnected, hackers have the opportunity to mount a number of attacks at a distance.

Threats to connected cars

Stealing personally identifiable information (PII) such as financial information, personal trip information, and location information

Controlling vehicles remotely, where a vehicle's operation is controlled by an external source

Making unauthorized vehicle entry, such as keyless systems using mobile applications or wireless key fobs

Compromising mobile application security, where poor application security leads to malicious attacks or compromised systems

Fortifying the connected car with application shielding

Application shielding is the process of adding security functionality directly to applications and other software so that they can withstand hacker attacks independently from the surrounding environment. It combines prevention, detection, remediation, and prediction to go beyond basic best practices, delivering the highest level of software security available today. Application shielding is ideal for high-value applications to prevent the crippling effects hacks can have on auto manufacturers when brand reputation, company trust, and human life are at stake.

Jailbreak and rooting detection
Prevents the application from running on jailbroken and rooted devices by employing a number of smart detection checks inserted into the code.

Diversification
Protects software against Break One Run Everywhere (BORE) attacks by ensuring every protected application is different.

Customizable defense actions
Configures protected applications to execute custom callback functions when particular threats are detected.

Business benefits

Cost efficiency
Integrating with Intertrust security products is faster, cheaper, and more secure than developing your own software security infrastructure.

Time-tested techniques
Intertrust solutions have been successfully applied to millions of devices to mitigate software attack risks.

Wide platform support
Our software tools support most operating systems, CPU architectures, and programming languages.

Brand protection
Build your brand and prevent loss of reputation by protecting your endpoints and managing risk with application shielding.

Up-to-date security
We closely monitor the latest security flaws and attacks, and constantly improve our products.

Global support services
Our distributed development and support teams cover the Americas, EMEA, and Asia-Pacific.

Intertrust products and services for connected cars

Intertrust provides trusted computing products and services to leading global corporations—from mobile and CE manufacturers and service providers to enterprise software platform companies. These products include the world's leading digital rights management, software tamper resistance and privacy-driven data platforms for digital advertising, marketing technologies, and IoT.

whiteCryption®
whiteCryption, a subsidiary of Intertrust, is a leading provider of application shielding solutions to prevent hackers from reverse engineering and tampering with code. Its application shielding portfolio consists of two products.

whiteCryption Code Protection™
provides application developers with a comprehensive suite of anti-reverse engineering and runtime application security features to help protect your applications. Code Protection is easy to use and requires no significant changes to the code itself or the existing build chain.

whiteCryption Secure Key Box™ is an
advanced white-box cryptography library that protects cryptographic keys for critical security functions such as device authentication, secure communication, and data encryption. With Secure Key Box, cryptographic keys are never in the clear whether they are in use, in transit, or at rest.

Learn more about whiteCryption at:
**intertrust.com/products/
application-shielding**

Seacert®
Seacert provides public-key infrastructure, specializing in large-scale device identity provisioning. Seacert supports device and PKI infrastructure with several services.

Public-key infrastructure (PKI)
PKI lifecycle services, including creation and management of root certificates and certificate authorities, certificate signing requests, and certificate revocation services. Seacert services meet the highest industrial quality standards certified to both Webtrust and ISO 9001 standards.

High-volume device identity provisioning
We provision millions of devices every day with cryptographically secure identities and authorization credentials. We provide both factory floor provisioning with bulk key delivery and field provisioning through our cloud-enabled provisioning services.

Custom infrastructure
Intertrust focuses on creating device identities that go beyond standard TLS/SSL certificates and employee credentials to meet the needs of the complex closed ecosystems. Our PKI experts work with you to design a management and delivery infrastructure that meets your unique needs.

Learn more about Seacert at:
**intertrust.com/products/
key-provisioning**

Features

whiteCryption®
Obfuscation
Makes the code appear obscure while keeping functionality the same.

Integrity protection
Prevents attackers from making any modifications to the application.

White-box cryptography
Provides strong protection for cryptographic keys.

Anti-debugging
Enables the application to identify the presence of a debugger.

Seacert®
Complete Managed Service
High volume service supporting offline and online provisioning

Security and Standards Compliance
WebTrust compliant and ISO 9001:2015 certified service

Custom PKI Services
Supported by a world class team of experts in complex custom PKI integrations