irdeto

Datasheet

Cybersecurity solutions for the pre-market: Defense in Depth technologies

There's a reason some front doors have a cylinder lock, a deadbolt, and a chain lock. It's layered security. If a burglar breaks through one, they're met with another hurdle. The same logic applies to employing defense in depth cybersecurity technologies for medical device software. If a nefarious actor cracks through one layer, redundant mechanisms have the potential to thwart a successful attack.

The risk to medical devices is changing. As connected devices proliferate out of the more secure space within managed networks and into hostile environments such as unmanaged networks and community settings with larger attack surfaces, the threat of a cyber attack grows.

Similar to the home security scenario described above, cybersecurity for medical devices is best accomplished with multiple redundant and layered defensive mechanisms, an approach which is being recognized as a state of the art practice by regulators and standards bodies alike.

Also driving the need for layered security is the CIA triad, a model commonly used in a variety of industries to guide cybersecurity strategies. The acronym stands for Confidentiality, Integrity and Availability, three principles used by security teams to establish priorities, identify vulnerabilities and guide risk mitigation solutions.

Irdeto's suite of multi-layered technologies both secures these core elements and helps device makers meet the state of the art cybersecurity requirements needed for market access.

BENEFITS OF IRDETO'S TECHNOLOGIES

Unlike many solutions on the market, our **cryptographic solutions** are software-based, making them easy to integrate and highly scalable.

Our **obfuscation solution** integrates directly into the product build process for maximum convenience, and the automated protections allow for rapid deployment of security capabilities.

Our managed **PKI suite** allows for efficient updating of keys, software and security measures in field deployments

IRDETO'S DEFENSE IN DEPTH TECHNOLOGIES

At Irdeto, our solutions facilitate a multi-layered approach to the protection of code, data, keys and intellectual property via technologies that have negligible performance impact on the product and no negative impact on the functioning of the device.

Enterprise-Grade Software Obfuscation

Software obfuscation is the modification of source code in a way that hides the details of the original software, preventing an attacker from analyzing or modifying the flow of execution to expose secrets or intellectual property and making it harder for attackers to confirm the presence of vulnerabilities. This can be a useful first layer of protection against criminals trying to develop an exploit against your application in order to access sensitive data or intellectual property.

As un-optimized software obfuscation can be heavy and require a significant amount of space in the execution environment and/or slow the processing speed of the software, Irdeto's approach to obfuscation is designed to reduce impact on performance critical areas.

Other benefits of Irdeto's solution include: it obscures key software decision points – even while they execute, protects critical application logic and functions from untrusted inputs, and prevents theft and alteration of valuable algorithms.

Irdeto's Cryptographic Solution

- Easy to integrate via API
- Software-based
- No special cryptography knowledge needed by your developers
- Irdeto developers do the work 'under the hood'
- Highly scalable

Whitebox Cryptography

Standard cryptography assumes that the endpoints and platforms are hosted in secure environments, essentially protected by a black box. More protection is needed in a hostile environment where an attacker may have the ability to monitor the application and extract keys which can be used to hack into the software.

Irdeto employs whitebox encryption. It works under the assumption that an attacker has complete visibility and access to the code and therefore keeps keys and data hidden along all points in the cryptographic computations.

Our whitebox cryptography can also be added to off-the-shelf hardware or inside an application operating in an untrusted environment.

While hardware-based solutions are platform dependent, a software-based approach such as ours is renewable, reusable and portable.

Platforms:

- Supported on all major desktop/mobile platforms

Black box attack

- Attacker knows algorithm
- Watches inputs and outputs
- Controls input text
- No visibility of execution

Gray box attack

- Attacker knows algorithm
- Watches inputs and outputs
- Monitors side channels, i.e. timing
- Controls input text
- Indirect visibility of execution

White box attack

- Attacker knows algorithm
- Watches inputs, outputs, intermediate calculations
- Controls input text and can alter intermediate data
- Full visibility of execution

PKI Services

Irdeto's public key infrastructure (PKI) technology helps ensure the availability, integrity and confidentiality (the CIA triad) of user data, device operations and security critical functions.

Our full suite of PKI capabilities addresses multiple use cases as well as secure physical environments where critical keys can be stored for complete protection and can adapt to a variety of security technologies for ongoing protection. This makes it effective for a variety of devices including devices with:

- Legacy designs
- Hardware constraints and commercial trade-offs
- Mergers & Acquisitions

PROVEN

- 350 million embedded devices protected, 1 billion PKI certificates issued, high scalability
- ISO 27001-2013 certified facilities with Irdeto professionals for safeguarding customer's assets

FLEXIBLE

- Hosted, with on-prem centrally-managed keying appliances
- X.509 PKI, code signing certificates, symmetric keys, debug passwords
- Wide support for HW roots-of-trust in devices (HSMs, TEEs, TPMs, Secure Elements)

OPEN

- Wide support for key management standards
- Support for major Hardware Security Modules brands
- Role-based authorization integrated with enterprise identity providers
- The customer retains ownership over all security assets (escrow) – no lock-in

Languages & platforms supported:

- Support for both compiled native code e.g. C/C++ and interpreted languages e.g. javascript
- Support for all major platforms, e.g. windows, macOS, Linux, iOS, Android

CONTACT US

For more information on Irdeto's Connected Health Cybersecurity Services and Solutions visit our website.

Or contact Lucas Catranis at lucas.catranis@irdeto.com

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.

Last modification: 18-11-2021 / 11:10 am GMT+01:00