



G+D Mobile Security collaborates with lowRISC to support OpenTitan, a new open source project

05-11-19

München

Giesecke+Devrient

Companies' aim is to make the hardware root more transparent, trustworthy, and secure for everyone.

Munich, November 5th, 2019 –G+D Mobile Security, a leading provider of connectivity and security in IoT, today announced it has partnered with lowRISC and Google in support of OpenTitan, an open source hardware root of trust (RoT) reference design and integration guidelines that enable chip producers and platform providers to build transparently implemented, high-quality hardware RoT chips tailored for data center servers and other devices.

Security begins with infrastructure, and OpenTitan will help ensure transparently implemented root of trust in hardware at the foundation level for a multitude of devices such as server motherboards, network cards, routers and IoT. Adopters of this framework can inspect and contribute to OpenTitan's register-transfer level (RTL) design, firmware, and documentation, helping to build more transparent, trustworthy hardware RoT chips for everyone.

As a leader in secure embedded software, G+D Mobile Security fully supports the vision of the OpenTitan project that hardware security should be open and transparent. The main motivations for G+D Mobile Security to participate in this landmark project are the company's proven track record of security and certifications as well as its experience in other open source projects. Albeit the benefits of an open and transparent hardware root of trust would be very beneficial to the rapidly evolving IoT ecosystem.

Key benefits of OpenTitan for chip manufacturers and platform providers include:

- ➔ **Transparency:** Adopters can inspect and contribute to OpenTitan's design, firmware, and documentation, helping to build more transparent, trustworthy hardware RoT chips that benefit everyone.
- ➔ **High-quality:** OpenTitan's goal is to build and maintain a high-quality and logically secure RTL design, firmware, and documentation. The project is staffed by expert engineers focused on rigorous design validation and technical documentation, all based on key learnings from designing Google's Titan chips.
- ➔ **Flexibility:** Adopters can increase their total addressable market and reduce costs by using a single platform-agnostic hardware RoT design that can be integrated in data center servers, peripherals, and any other hardware platforms.

"It is a privilege for G+D Mobile Security to be part of this landmark project," says Carsten Ahrens, CEO of G+D Mobile Security. "We are fully committed to making OpenTitan the first Open Source RoT hardware platform that will be certified to meet the requirements of all cloud and IoT security use cases."

"At lowRISC, our mission is to establish a vibrant ecosystem around open silicon designs and to help lower the barrier to producing custom chips," said Gavin Ferris, lowRISC CIC board member. "Creating an ecosystem of like-minded organizations focused on the goal of improving transparency around chips helps increase trust in the overall security of the infrastructure on which software runs. With OpenTitan, enterprise organizations and consumers alike will benefit from services built on a more secure infrastructure that is anchored in transparently implemented OpenTitan chips."

"Customers are asked to put faith in proprietary hardware RoT chips for their mission-critical systems without the ability to fully understand, inspect and therefore trust them," said Dominic Rizzo, OpenTitan engineering lead at Google Cloud. "By creating OpenTitan with the broader hardware and academic community, we can leverage the experience and security principles used to create Google's own Titan chips to make hardware RoT designs more transparent, inspectable, and accessible to the rest of the industry. Security should never be built on opacity."

OpenTitan is managed by an independent organization, lowRISC, which is a not-for-profit engineering company that uses collaborative engineering to develop and maintain open source silicon designs and tools for the long term.

About G+D Mobile Security

G+D Mobile Security is a global mobile security technology company headquartered in Munich, Germany. The company is part of the Giesecke+Devrient group. G+D Mobile Security has a workforce of 5,300 employees and generated sales of EUR 868 m in the 2018 fiscal year. More than 40 sales and partner offices as well as 20+ certified production and personalization sites and data centers ensure customer proximity worldwide.

G+D Mobile Security manages and secures billions of digital identities throughout their entire life cycle. Our products and solutions are used by commercial banks, mobile network operators, car and mobile device manufacturers, business enterprises, transit authorities and health insurances and their customers every day to secure payment, communication and device-to-device interaction. G+D Mobile Security is a technology leader in its markets and holds a strong competitive position. For more information, please visit:

<https://www.gi-de.com/de/de/mobile-security>