May 7, 2020 | Steve Atkins | 0 Comments

Maintaining license security in the time of COVID-19

Interview with Oliver Winzenried, CEO & Co-Founder of Wibu-Systems

During the enforced COVID-19 lock-down scenario that Germany found itself in recently, the Silicon Trust reached to out Wibu-Systems to find out how they were doing during this difficult time.

Silicon Trust's Program Director Steve Atkins spoke to CEO and Co-Founder of Wibu-Systems, Oliver Winzenried over a video conference and asked his opinion on subjects such as security, digital transformations and the Industrial IoT revolution and how the current state of the world is impacting these topics.

Steve Atkins: Let's begin. Seeing how the Coronavirus pandemic is disrupting business, causing mass unemployment and changing everyone's lives, do you think that this global emergency is changing the pace of digital transformation?

Oliver Winzenried: I think that the speed of the digital transformation is increasing; I am seeing many changes with a positive outlook. Nevertheless, we'll continue to focus on our vision of protecting digital assets. I think the role of software in smart working is increasing in many areas. For example, in big data analytics and analysis, for controlling the spread of the disease, or software for engineering and other applications within the smart working area. Within these areas, security plays a more important role than ever before.

We are also seeing an increasing number of cyberattacks and the increasing presence and activities of online cyber criminals, as they take every opportunity that is presented to them thanks to increased mobile working. Because of this new scenario, security is increasingly important in all applications and devices – especially medical devices with their firmware and device settings and the handling of patient's medical data.

With our solutions, Wibu-Systems is co-operating with many medical device manufacturers, for example Fritz-Stephan GmbH in Germany who are producing (in three shifts now) emergency ventilation units. With Agfa HealthCare, with United Imaging who are doing computer radiography equipment, and with Metrohm Healthcare for their high precision medical instruments and Agilent Scientific Instruments for clinical diagnostics custom-made for cardiological solutions. So, we are working with companies creating many applications in this medical field.

In spite of social distancing, of course, people are staying connected with the aid of today's telecommunication possibilities – which is a great help. However, there are also other factors to take into consideration that can make working in today's climate more difficult. For instance, in our company, with its many IT and development tasks and so on, people can work mobile and from home. But it is not always efficient, because even though we have collaboration tools for the agile development teams, it is not always the same as meeting around the table to develop solutions.

https://silicontrust.org/2020/05/07/maintaining-license-security-in-the-time-of-covid-19/

Even though it is possible for us, there are many other tasks in many other industries where people are not that lucky and can only do their work when they are physically present. In today's scenario, that may require a lot of re-organisation. Many production facilities have been closed – although I believe they are slowly starting up again (in China, they are more-or-less up again) – and logistic companies have also required people to be physically present to continue to operate. These companies and industries have many tasks that cannot be performed from home. So that is a big challenge for them, not to mention the challenges that individuals are facing at the moment when they are working from home while they are also having to take care of their children.

At the end of the day, though, there are increasing security demands due to these changes. With our customers (and their end users), their products are working with software that usually requires validation from an installed license server. If their employees are working from home, they may not necessarily have a sophisticated enough VPN solution to access the license server and may face difficulties. So, we did a little bit to help and ensured that our new CodeMeter Cloud Licenses (the licenses are really stored in the cloud) could be accessed without any special VPN requirement – just a normal internet connection. We are also providing this cloud container for our ISVs – where they currently have home office users – for free in this period of time. Currently, we have this offer up until the end of the first half of the year, and we will see what we can do after that.

SA: What critical factors can make the industrial IoT revolution position itself as a beacon of light during these gloomy days we find ourselves living in?
OW: I think it is very important to maintain trustworthiness and reliability. IoT and connected devices are used more and more – in factories, in machines, in cars, in many automotive applications, in many medical applications, and in smart homes as well. They provide big benefits, but they can be subject to massive cyber-attacks and other risks of failure.
They can fulfil their tasks reliably and correctly only if security is implemented in the correct way.

Security, on the other side, is never 100%, we know that. And the more complex the systems are, the more we should ensure that they are working correctly, and that is where the secure element (SE) comes into play. Secure elements are small systems with reduced complexity that do some cryptographic operations, key storage, and some security operations, but it is only a small part of the total system. Due to their low complexity and their small size, they can be deeply evaluated, they can be certified. And I will not say that they are proven free of any bugs or failures, but the security level is really high.

These secure elements as an anchor of trust are really necessary to be integrated in all of these IoT devices.

SA: So which secure elements does Wibu-systems offer to facilitate this digital transformation and what are their specific characteristics?
OW: Our secure elements we call CodeMeter dongles. They are available in different form factors and in many different physical interfaces. The heart of our secure elements of our CodeMeter dongles is a security controller that is Common Criteria EAL5+ certified, and there is also a certified crypto library in our security controllers (made by Infineon Technologies). What is special is that they are designed and qualified for an extended

temperature range for extended environmental conditions, where they can be used in automotive, in industrial automation, or medical applications. That's one specific thing compared to products that are designed and made for the consumer market.

On the other side, as well as multiple interfaces, they offer not only key storage and basic crypto operations, but they provide the full CodeMeter solution. That means they have large secure memory to not only store a number of certificates and keys, but can do flexible licensing and store all the license conditions that are specified and defined by the ISV or device manufacturer. This flexible license management helps manufacturers realize new business models and also create new protection levels through our back-end Blurry Box technology, which was awarded the German IT security award a few years ago. Many of these schemes are implemented in our secure elements as well. So, it is much more than just key storage or certificate storage – it is a secure element that offers the full CodeMeter functionality, integrated in the CodeMeter world.

The interfaces are not so interesting – every knows them. From the consumer market, there are SD cards that look like normal memory cards or compact flash cards that look like normal consumer compact flash cards. What we always have in our CodeMeter dongles is this secure element that provides this high level of security for all these operations.

SA: In terms of functionality, which purposes do all these different secure elements serve?

OW: Our company slogan is 'Perfection in Protection, Licensing, & Security', and this is what we offer, what the total CodeMeter solution offers. First, secure protection means protection against counterfeiting, protection against reverse engineering (so it protects the Intellectual Property of a software or device manufacturer). Second, secure licensing means that they can realize new business models, and they are flexible to realize many, many different license models; perpetual licenses, named licenses, floating licenses in the network, pay-per-use mechanisms, feature-on-demand, subscription licenses, trial licenses, expiration dates, maintenance periods, and many more. So, it is licensing with high flexibility. The last topic – security: this refers to tamper protection and cyber-security protection against cyber-attacks, and that is enabled with the Common Criteria Certified security controller inside, allowing certificate storage. In conjunction with the CodeMeter infrastructure and the back-office systems, such as the License Central, we also offer the solution for the easy and secured deployment of certificates.

We are not going into the authentication business, because that is a completely different customer target group. We are providing this solution for our customers, device manufacturers, and software vendors. They can get a double benefit from our solution, because they can do IP protection with flexible licensing, and they can give their devices and software a secure identity. They can provide secure updates, and they can use all the mechanisms where certificates are used today.

Let me explain one more example with our secure elements. We have our CodeMeter dongles (and also with flash disk) that come in the USB memory stick format that everyone knows. If you have a flash disk (a semiconductor disk), you can store data on it, but you cannot really delete it in a secure way. This is because, on such a semiconductor disk, there will always be faulty memory cells. The user takes no notice of them, because they are automatically sorted out (they tend to be called 'bad blocks') and will never be used by the files or the

operating system. But information that is written to these bad blocks can also never be deleted, even with a re-formatting of the flash disk. And with certain tools, you can access and read these 'bad blocks'. Therefore, these 'bad blocks' are a fundamental risk in many applications using standard flash disks. With our CodeMeter dongles and flash disks and SD cards and other user interfaces, the data that is written to the private partition of the disk is encrypted and a key is provided by the security controller – so deleting this is very easy. You don't need to delete the data – you just need to destroy or delete the key, and then all the data (even in the 'bad blocks') is of no value anymore. This secure deletion is one of the key features of our CodeMeter dongles with flash disks.

SA: Thanks Oliver. Let's wrap up this short conversation with a closing thought: what are the USP's of Wibu-systems, and how can they better the world?
OW: I would say that what we need today, with increasing connectivity everywhere, is something like an 'anchor of trust'. This anchor of trust can be realized in a highly secure way with our secure elements, with our CodeMeter dongles. Of course, we are not providing the end user applications – we are providing our solutions to the intelligent device manufacturer or to the software vendors (they integrate it), and they get all the tools and the mechanisms from us to realize that.

Looking to our USPs, we talk about forward interoperability, and that means that our license containers are interoperable, and they can be stored in a very highly secure way in our CodeMeter dongles – the secure element that we talked about during this conversation, but they can also be stored in a software license, with so-called activation in a CmActLicense, and they can also be stored in the cloud. In the same form and completely interoperable with no change to the protected product needed, and no change to the deployment and business process needed.

The next point is that we can support, in an interoperable way, almost any kind of device, starting from small microcontrollers to embedded systems to standard PC, and server systems using x86 architecture, ARM, MIPS, PowerPC. And applications are possible in microcontroller-based products, in embedded products, in PLCs, in PCs, in servers, to software running in the cloud.

Then we support multiple platforms, that's number three. So, multi-platform support includes different operating systems like Windows, LINUX, Micros, but also a wide variety of operating systems like UNIX or VxWorks, and they can be applied in PLC systems, or they can be used with native code or used with .NET and Java as well.

My last point for forward interoperability concerns back office integration, because all these mechanisms need to be integrated for manufacturers in a way that is complimentary with their business process. License creation, key creation, and deployment should be connected to their SAP system, their e-commerce platform (whatever they are using). And with our CodeMeter License Central, we can integrate these tasks in a variety of different business processes that vendors have and give them a great amount of freedom to choose what fits best for their application and for their business. That is something that is really important.

What can we do to better the world? That's a good question. I think all these mechanisms help and create win-win-win situations. You can only ever look at examples – we have a nice example of a manufacturer of computer radiography equipment that provides and installs computer radiography equipment in hospitals in India at a low fee and does a pay-per-use or a monthly subscription-based business model with the hospitals.

That creates benefits for all. I think it creates benefits for the medical device manufacturer, through the higher quantity of devices and machines. It creates benefits for the hospitals that would not be able afford the normal investment. And it creates benefits for the people living in the area of this hospital, because if their diagnostic system is not available there, they cannot get this high-quality diagnostic in case they need it. We have supplied our CodeMeter Cloud home office license for ISVs for free.

I don't know how long it will take to recover from this situation. I am quite sure that it will take many more months, and it will have implications and affect every corner of the planet. I am sure that things are happening differently in different areas – we see China where the demand for our products is still at the pre-Corona level. Their manufacturers are working again. In different parts of the world, step-by-step, everything will recover after the health situation is better.

SA: Oliver that's fantastic. We appreciate you talking to us. All the best, stay healthy and I look forward to seeing you in person very, very soon
OW: Thank you Steve – same to you.