
# What Works in Certificate and Key Management: Enabling Secure Digital Business Using Venafi's Trust Protection Platform

*SPONSORED BY*

VENAFI®

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

Encryption of data in motion with SSL and VPNs, as well as encryption of data at rest, can be high value in raising the bar against attacks looking to capture or compromise the integrity sensitive information. However, doing encryption badly can lead to self-inflicted wounds through a false sense of security or disrupting legitimate business when PKI certificates expire or are revoked. Processes and tools to manage encryption keys and certificates are needed to enable secure business and maintaining high service levels.

Troels Oerting, Chief Security Officer at Barclays Bank will provide details of his selection and deployment of Venafi to enable discovery and management of encryption keys and certificates in use across Barclays, supporting more transparent use of encryption, avoiding business disruption from expired certificates and demonstrating benefits to increased integrity and availability of critical business processes.

## ABOUT THE USER

Troels Oerting is the Head of the World Economic Forum Centre for Cybersecurity established by World Economic Forum in 2018. He has been working in cybersecurity 'first line' for the last 38 years and has held a number of significant posts both nationally and internationally, and has an extensive network covering both public and private institutions. Before joining World Economic Forum, Troels worked as Group Chief Information Security Officer (CISO) and Group Chief Security Officer (CSO) with end-to-end responsibility of all security in Barclays Group, and was responsible for more than 3000 security experts world-wide protecting banks.

## ABOUT THE INTERVIEWER

John Pescatore, Director of Emerging Security Trends, SANS Institute

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

**Q Give us a little idea about your background and your position at Barclays.**

A I am the Chief Security Officer at Barclays, and my background is a blend of law enforcement and intelligence. I've been a Chief in the Danish police and worked at the Danish equivalent of the FBI operating department. I've been an assistant director in Europol, the collaboration in the European Union. I was also the implementer and First Chief of the European Cyber Crime Center. I then joined Barclays, where my responsibility is broader security. At Barclays, we don't talk about information security or cybersecurity—we just talk about security. And it's my role to make sure that our 50 million customers and 142,000 employees remain relatively safe for everything they do online and offline.

**Q As the CSO at Barclays, do you report to the CIO or how is security in the organizational structure?**

A I report to the COO at Barclays.

**Q Given your background, and since some of the things Venafi's products do, are you involved in the fraud side of financial transactions, or is it all the security side?**

A Yes, I'm responsible for fraud prevention as well. My mandate is security by design. So, I need to make sure that anything we do keeps security in mind before, during and after a transaction. So, I think it's a rather holistic and broad role.

**Q Since this case study is about what works around your selection and use of Venafi products, what sort of business problems or threats were out there that prompted you to look for this kind of solution?**

A I think that in all banks, you have a great need for certificates and keys, especially taking into consideration that we spend much money and time controlling human access to IT systems, platforms and applications. But, in the future, we will need to look at how we actually secure machine-to-machine communication as well as communication using certificates. We will also need to consider how we make sure that our keys are always valid and that they always are up to date.

At Barclays, we have a strong encryption organization. So, we create our own certificates using extremely skilled people under heavy security policies. But, we realized what we needed was a better way to administer and optimize this process. That was why we started looking into what kind of companies and tools could help us streamline these efforts. Our goal was to increase our efficiency around the use of certificates, and to make our use of them much more transparent. First of all, we wanted to be safer, and secondly, we didn't want to have any technical problems caused by expiring certificates, which sometimes can have a tremendous impact on business. That was the background for the search of such a system, and that's where Venafi came into the equation.

**Q Can you give us any idea of the scale of Barclays Global? Is it hundreds of thousands of certificates?**

A It's amazing. Barclays is one of the biggest banks, and I suppose, like any other bank, a very complicated bank that has grown rapidly by acquisition. So, we were managing hundreds of thousands of certificates that were operating in all kinds of forms and shapes all over the globe. To keep that on track and to avoid problems that keep you up at night, we knew we needed a more advanced approach to managing our use of certificates and encryption keys.

**Q You said you had an encryption organization; so you were generating certificates internally. I assume you had SSL certificates for web servers? You mentioned machine to machine. Did the problem include other things, things like SSH or VPN?**

A All of that. Our philosophy is that anything that moves on our system needs to be secured in the highest possible way. So, we were deploying certificates for VPNs as well as SSL and ssh. We decided to make sure that we took all of these use cases into consideration when we looked into solutions.

**Q What process did you use? Did you start looking around to see what type of products there were? Did you look at developing a solution yourself? Did you put out an invitation for bids or tenders and request for proposals, or how did you go about looking for a solution?**

A Vendor selection is one of the crucial areas where companies struggle, especially with vendors who want to provide something. As a CSO, I get more than 200-300 emails every day from companies who have a good product—a "silver bullet" to offer. First of all, I don't believe they do have that, and secondly, it's a big game of clones, and thirdly, it wastes so much of my time if I have to go through all of this mess.

So, in this area, CSOs can either use their network or run a network exercise through the organization in order to short list those who seem to be the best providers in any area. If you're looking for insider input on this kind of tool, you would look internally first to make an estimation of who is good. Then you'll make a short list of trusted resources, and engage with a few of them, depending on your appetite and your time.

This is one of the crucial areas that I think companies struggle with, especially since there are so many vendors trying to get access to CSOs. I've found the most efficient way is to use my personal network of CSOs and well as others within Barclays to build a short list of those vendors who seem to be the best providers in any given area.

In this case, several people in my organization, including the head of our crypto department, recommended that I speak to Venafi. Based on that, I had a meeting with the CEO of Venafi and we took the next steps. Normally, we would do an internal assessment where we use all kinds of input, from SANS or Gartner, and others. But, in this case, it was a bit different because there just aren't many other turnkey products in this area

**Q So, how did you get started? Did you pick one application and then start small and do a proof of concept? How did you get going?**

A I felt that if we could more effectively manage certificates and keys, we had an opportunity to increase security in an area that, on the surface, seems rather dull and rather boring, something that is under the hood that nobody really sees. To do that, I was looking to do more than just buy a product and have our team try it out. I instinctively got the feeling that we needed to create more than a customer/vendor relationship, we had to engage in a real partnership. I think that we were so big and so good at what we do that we needed to engage in a two-way street. In other words we need a partnership where we had significant influence on how the product actually works, how we can configure it, how we can use it to do more, where we can provide advice on how to improve it. That was the discussion I had with Venafi and they were very open to this type of working relationship.

Once we had established that partnership, I said to my guys, "You should now engage with Venafi and you should explore areas where we can get a quick win. Define areas for more long-term investment and then come back to me with a recommendation on how we should approach it." That was the bottom line—develop a partnership in this field that will grow over time, so that we could get it implemented in the way that best suited us and the company.

**Q From a timing perspective, how long ago did you start using the Venafi solution?**

A The start of our rollout was in 2015.

**Q The area of certificate management often crosses organizational boundaries. Within your security organization, who actually was in charge of this, and what other groups were involved?**

A At Barclays, we are rather inclusive. And while that approach has certain benefits, it can also increase the time to implement because everybody needs to be heard. But, in this situation, we gave my encryption team, which is located in Manchester, primary responsibility, but we did not do anything without having the infrastructure guys on board. So, the whole CIO organization was fully engaged. All the specialty directories needed to be involved. So, the head of the encryption team established a work group that included the business units, infrastructure services, network services and security management. Venafi was also part of that team.

We made sure that every time we had a touch point for any of these services, we covered it directly in the meeting. Or if not, we would follow up. We made sure that the implementation, and the use cases were realistic, and that they would deliver the expected results without any surprises—we wanted to be really prepared. After this solid preparation, we were able to execute rather fast. A common issue with Barclays is that it's so big, that software tools can have problems scaling to support our organization or our networks. But, in this case, we managed to scale without any big problems.

**Q With user certificates, it quite often turns out they're being used all over the place and often by third-party services. Did you have to do a discovery phase to find all the potential uses of certificates and keys?**

A Yes. I think we had such a good beginning and built such a good basis because we had a dedicated team which was extremely skilled. We had a very good view of where the keys and the certificates were located, when they would expire, how they were being used, who used them, and for what. In the past, we've had lots of trouble with third-party certificates that expired unexpectedly for one reason or another, so we

knew our problem areas. I don't pretend that it was perfect, but we had a rather good overview. Also, the integration or planning process included optimizing our databases where the various certificates and keys were used.

**Q Since deploying any product requires spending the company's money, were you able to capture any metrics of business benefit or any way to say "we made this investment and here's how it's helped the business"—were there any sort of measurable metrics you'd show to your boss, the COO or anybody else?**

A I think that's a good question because budget is what we're always constantly challenged with, especially for more strategic investments that aren't just a reaction to the latest threat. When I sold this solution to my boss, I convinced him that this is an area that is highly important now but will that it will increase in importance in the next couple of years as Barclays gets more involved in new technologies like the Internet of things, for example. When I made that decision back in 2015, I had to project how many more certificates we would need to manage and then convince management that this was an area that we need to be investing in. I drove the discussion to be more about the long-term business need, rather than short term it "will cost us so much or so little."

**Q Now that you are a couple years into this; knowing what you know now, are there any things you'd do differently or any lessons learned you can pass on?**

A I think that our approach was reasonable and that our focus on partnership gave us a stability that has been very beneficial. Venafi has proven that they are here to help us if there is anything that seems to go wrong. That peace of mind is something that you cannot measure by sales people and four-color pamphlets and whatever. It was a lesson we already knew, but I think that any business-critical security project should be based on this kind of partnership approach, with strong commitment from the vendor.

**Q What types of support are part of the partnership? Is it strictly product level support? Do you pay for onsite Venafi people that are part of your team? How does that work?**

A What was important for me, was that the service agreement would ensure swift support. I also needed the ability to deploy experts that sat next to my guys to fix whatever was needed—to actually be there and make sure that we got the real-time support that we needed. Venafi has done that. I don't believe we have had many occasions where we needed to use the onsite resources, but when we did need it, they've been there.

**Q Are there future initiatives you see extending your use of certificate and key management?**

A Technology now is moving so fast, and the devices that we need to support will be smaller, the batteries will last longer, and there will be sensors all over. We will be using the Internet of Things much more, as will all banks, because we will be forced to be where the customers want us to be. Everybody wants security and privacy, but most of all, our customers want convenience. So, it's all about creating a flawless customer experience without compromising security and privacy. In order to do so, we will need to secure machine-to-machine authentication and deploy encryption in all the areas where we will never engage with a human being.

I think that securing keys and certificates is an area that will boom and will become increasingly more important for businesses to succeed. Those who have not taken the same measures that we have early will have to scramble to catch up very, very fast. For example, with PSD2 (Revised Payment Services Directive), aggregators will have access to your APIs to obtain your customer information, and all that will be automated without human intervention. That is why it's so important that we get the security infrastructure right.

**Q Is there anything you'd like to bring up that I didn't ask about?**

A I think securing and protecting keys and certificates is an area where we need to explore more, we need to learn more from each other. Both crime and nation state activities on the Internet will continue to surge, and we need to be very, very sure that we can keep the sensitive information that we're entrusted by our customers safe. I think that trust will be a competitive differentiator for the future, not just for banks but for everybody else. In order to keep that trust, we need to make sure that all areas of our huge network are safe and secure. Encryption and certificates are a critical foundation for that.