

# CoreStreet Cuts the PKI Gordian Knot

Authentication is the foundation of all identity based computing, and public/private key technology forms the basis of many identity techniques. But Public Key Infrastructure (PKI) has struggled to provide its promise of credentialed authentication. Large scale, widely distributed, real-time PKI validations tend to be too slow, and the infrastructure to support them problematic to deploy. CoreStreet has developed an innovative approach to the problem and the experience of their early customers indicates they have made real time PKI based authentication practical in applications where it previously wasn't.

**I**n a networked world, distributing the use of a fundamentally hierarchical architecture bogs down at scale, and large scale, cross-boundary PKI has been hampered by its rigorously hierarchical design. Finding solutions to this dilemma has been a fundamental pursuit of identity technology. CoreStreet has leveraged the work of their Chief Scientist, Dr. Silvio Micali on zero-



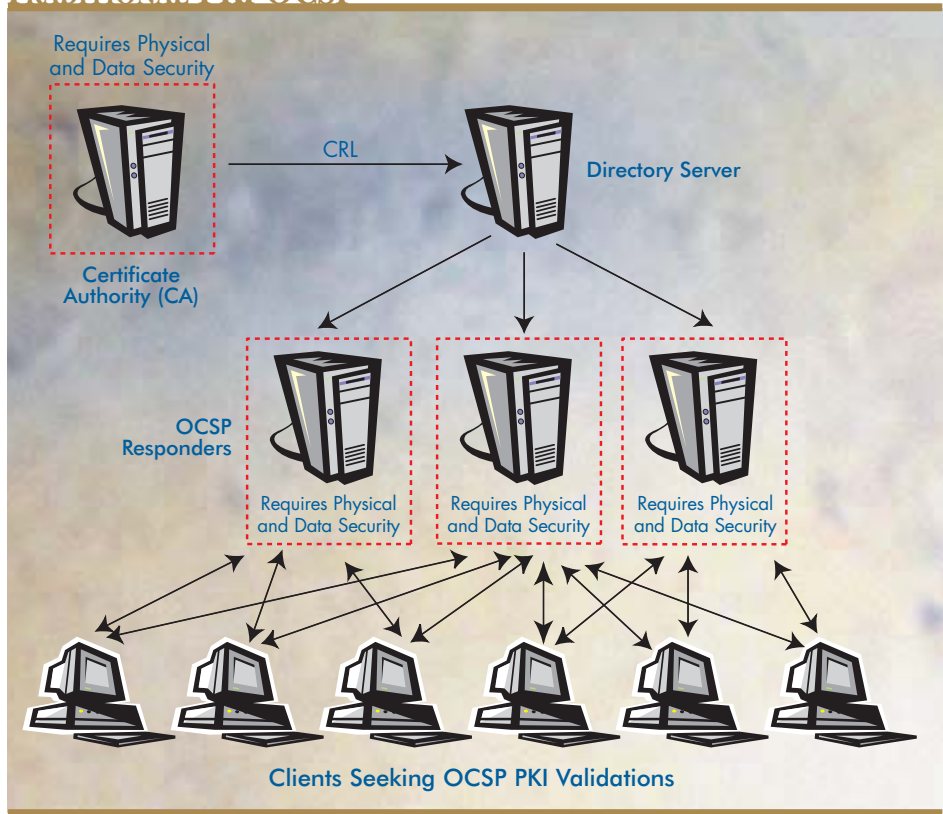
knowledge and interactive proofs to create a new architecture to propagate PKI that they call Real Time Credentials. Their approach can interface with standard PKI Certificate Authorities and deploy massively scalable validation systems with rapid response and lowered cost and complexity.

The heart of CoreStreet's technology is something they call a self-validating proof. These proofs are short messages that can be formulated in multiple ways to determine who is authorized to perform a specific action, and when. The cryptographic techniques that underlay these proofs allow rapid calculations, and prevent the messages from being forged, or modified by an unauthorized party. Because the proofs themselves carry no secret or sensitive information, they can be trusted even if distributed to unsecured media or over unsecured networks. This eliminates much of the cost and complexity of traditional large scale PKI.

### Understanding the Problem

A significant issue with traditional PKI is scaling the ability to rapidly prove that a credential is still valid at the time it is being used – especially if it is being used in a physically insecure location. Moving X.509 certificates around and verifying their authenticity isn't overly difficult, but PKI is designed to issue certificates with an expiration date that tells you a certificate is still valid unless it has been revoked before it expired. Thus you must either use short expiration dates and issue new certificates frequently (not realistic in large scale applications) or check with the CA on every use to see if the certificate has been revoked. Thus, to use a PKI certificate for authentication, you must either download a current Certificate Revocation List (CRL) and verify that the certificate you are checking isn't listed as invalid or make real-time inquiries to a PKI server using Online Certificate Status Protocol (OCSP).

### TRADITIONAL PKI OCSP



As PKI systems scale to very large numbers of users, the CRL will grow very large as certificates are revoked when people's credentials change. Scaling to handle large numbers of real-time OCSP inquiries is extremely expensive and creates significant physical security issues for servers in the structure since each OCSP uses a private key to sign its responses which must be physically protected from compromise. This has made traditional PKI expensive in many large scale applications, and simply unusable in others. For example, the U.S. Government has spent over \$1 billion so far to scale their PKI infrastructure to handle a few million certificates. For the DoD system, the CRL is over 20 megabytes and takes 15 minutes or more to download at remote sites with dial-up or slow network links. This makes using PKI to do things like validating email access on opening too slow to be useable.

### How CoreStreet Transforms the Problem

CoreStreet's technology allows the cur-

rent status of all certificates to be posted in network edge servers with low physical security requirements, creating the ability to scale a real-time inquiry methodology to validate certificates. CoreStreet simulates the OCSP structure with a single Real Time Credential Authority (RTCA) that is co-located with the PKI Certificate Authority. This RTCA generates proofs representing all possible OCSP responses and propagates these proofs to Real Time Credential responders that are distributed throughout the network. The RTC responders then act like OCSP responders in traditional PKI. What is different about the RTCs, however, is that they simply serve up the proof data fed to them. They don't have their own signing keys, and thus don't require the physical security that traditional PKI OCSP responders do.

The ability to distribute proofs to unsecured network edge servers has led CoreStreet and Akamai to team up to provide a massive scale global PKI vali-

dition infrastructure. George Economou, Product Manager for the Public Sector at Akamai said, "Core Street has intellectual property around running validation in a distributed manner without the traditional very costly requirements of having vault level security, armed guards etc. around the actual infrastructure that handles the validation. There are still requirements for that at the central location but they [remove] the security requirements from the infrastructure and validation, and that separation allows Akamai [to be used.] We have servers on over a thousand networks worldwide so we can provide almost an instant global distributed infrastructure that's scalable, high performance, and managed to support the application instantly."

## Real World Results

Last year the DoD did a pilot test of CoreStreet's Akamai enabled technology to compare it to traditional PKI for the Common Access Card project. They found that a validation took about 80 milliseconds using CoreStreet's technology compared to many minutes using traditional PKI and downloading CRLs. In the process of that pilot, the credential proofs for millions of Common Access Card users were distributed to the Akamai servers where other PKI enabled government applications could start to use them.

Silanis Technology, Inc. makes products to automate the business approval process using digital and electronic signatures. The government is a large user of their products and they were able to leverage the Akamai distributed Real Time Credentials. We asked Tom Petrogiannis, President of Silanis, how the CoreStreet solution affected their product use in the field.

"What we do is eliminate the need for people to go to paper to transfer information from one division to the next," said Petrogiannis. "They can keep it all electronic, routing it with something as simple as email or using work flow or using pure web based solutions. We've deployed to multiple departments within the DoD. Probably our most prestigious account is the Joint Chiefs of Staff, [but] they aren't really a large user in terms of the number of users - about 1,500 users. When we deployed to the US Army Medical Command they were north of 40,000 users worldwide, at over 110 locations. They've been using our technology for years to automate the process for everything from blood tests to sick leave."

"Our applications utilize PKI [and] before CoreStreet there was a real lack of ability to do real time validation. The current DoD CRL has cracked 30 megabytes. Because there are a couple of CRLs that have to be downloaded from a couple of central servers [a user] could wait as much as ten to fifteen minutes before they could actually perform an operation while that CRL gets cached. What that meant is [that] before Core Street in our applications we wouldn't actually check. We would allow you to sign a document and when someone would receive that document they could verify it after the fact to ensure that you really weren't revoked at the moment of signing - which really doesn't deliver on the full promise of PKI and security."

"With CoreStreet," continued Petrogiannis, "that problem is now eliminated. So we can turn on the ability to validate at the moment of approval and within tens of milliseconds, it comes back and says you are ok, you can be part of the network and you can go ahead and approve this document, or you've been revoked and you can't proceed any further. So they solved the

fundamental problem and enabled the full benefit of the PKI infrastructure to really shine through to the application layer where we are."

To illustrate the impact of real time validation, Petrogiannis gave this example. "To nominate someone for an award and to issue an award to the enlisted officer there are multiple people that have to go through the decision chain to approve that process. However, an award is critical to an enlisted man's career path and you want to ensure that those aren't fraudulent - that the people who approved them had the authority to approve the decision to grant the award."

"[Before CoreStreet] quite often they bypassed the DoD PKI because it was too slow to actually validate the credentials. The person's credential would be embedded in the form [and] travel with it so you have the audit trail of who signed it, but when they were actually doing the approvals, there wasn't any real time checking to ensure that you were the officer that you said you were and that you were still part of the DoD. [The award] would go through its process for a few days and at the end somebody would have to do a QA on the final form and check the credentials of every person who signed that off. That would be the poor soul who would have to download the CRL, wait fifteen minutes for it to get cached on their system, and then go through and validate the credentials one by one in the form that they received. Still better than paper, but nowhere near the efficiency that the full PKI would give you if you had that all electronic and [were] able to leverage the real time validation."

"What [happens] now, when the Core Street infrastructure is part of the solution, that validation of the user [happens] at the moment of signing in mil-

## HOW CORESTREET SEPARATES SECURITY FROM NETWORKING

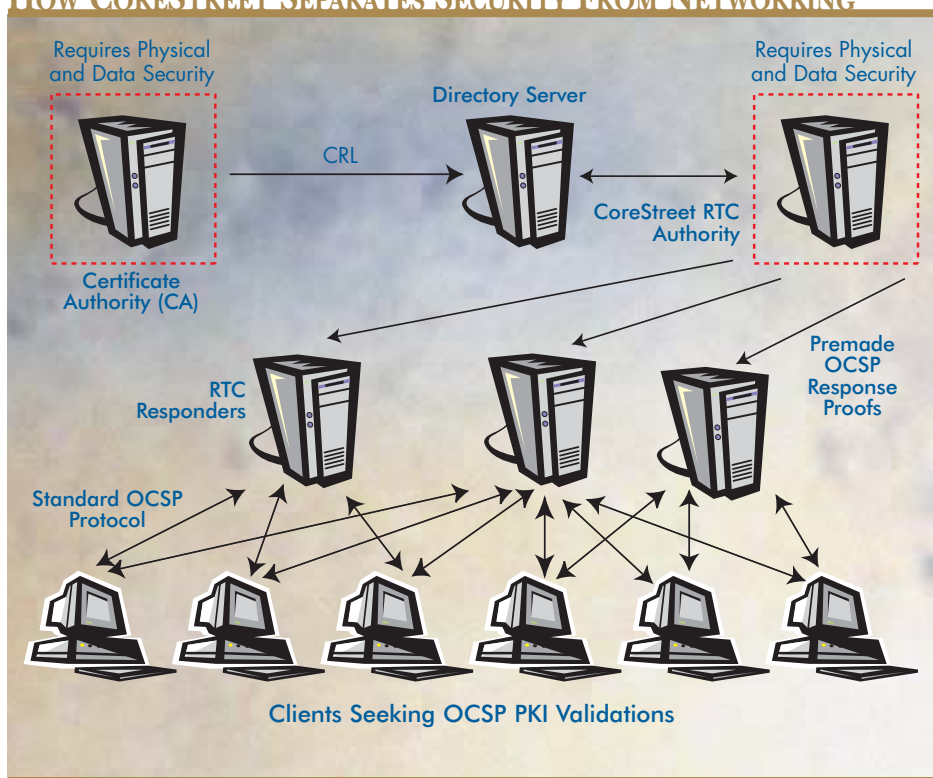
liseconds. To the end user they see no difference [from] what they were seeing before using our technology alone, but the need to QA it at the end of the process is eliminated because it's happening as the process continues. If someone was revoked from the DoD PKI with Core Street in the equation they would be prevented from actually approving, so you couldn't introduce bad data into the decision process."

### Off-Line Validation and Physical Locks

Traditional PKI must be online to validate credentials, making its use for physical locks expensive. The CoreStreet technology allows a transformation of the authentication and authorization process that allows smart card access to be validated off-line. An offline reader needs a policy defining access for users or user groups and the public certificate of the RTC Validation Authority that issues the proofs. This is all information that doesn't need to be kept secure, so putting it in a remote, unconnected lock doesn't present security problems.

On each smart card key, a proof is written that is valid for a specific time period. The off-line reader can then validate that a smart card is authorized and has access rights to the lock. If the proof is out of date or doesn't match the policy in the reader, the user is denied access. The only issue with such a system is how to get the proofs written to the smart card each day. This can be done by having network attached readers at the entry points to the building which updates the card with a current proof upon first entry.

Assa Abloy is the world's largest lock supplier providing brands such as HID, Yale, Sargent, Rixson and others. Assa Abloy will embed CoreStreet's Real Time Credential technology into door locks for access control validation.



According to Assa Abloy, their CoreStreet enabled locks will be the world's first physical access system that provides real-time authentication, revocation and auditing for wired, wireless, and even totally disconnected environments and should become available in quantity within the next year.

Göran Jansson, Deputy CEO, of Assa Abloy said, "In the last 25 to 30 years, access control has started to be delivered through electronic access control using cards, which is very convenient. It's very reliable and works very well. But it is quite costly to wire all these doors we have, and today maybe 5% of all doors are wired and have access control. How can you actually get a bit of both worlds – the convenience, logging, the ability to revoke and update certain remote locks without spending all this money per door by wiring them? This is a dilemma that we've solved to a great extent with this credential technology. The cost [of a CoreStreet enabled lock] will be between 10% and 20% of a wired solu-

tion. I think one still will probably use a wired solution for the doors where you have more frequent openings, but for the more remote doors where you have less frequent openings, it makes sense to not spend the same kind of money. [And] there is convergence with IT security. You can use the same token both to open the door and give you access to the system. By doing that you also enhance administration by doing it at one point."

### A New Approach to An Old Problem

CoreStreet has created a new approach to the long standing problem of PKI use in the real world. They have shown that their technology works, and are partnering to make it even more widely applicable to more problems. In handling the problems of PKI deployment at large scale and the problems of physical security in wireless or detached modes, they are tackling two of the major barriers to PKI use, and are working to show that PKI can yet become much of what it promised. ■